PROTECTING HEALTH INFORMATION: LEGISLATIVE OPTIONS FOR MEDICAL PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

MAY 19, 1998

Serial No. 105–179

Printed for the use of the Committee on Government Reform and Oversight

U.S. GOVERNMENT PRINTING OFFICE

52–018 WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-058318-7

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
J. DENNIS HASTERT, Illinois
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
CHRISTOPHER COX, California
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. McINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
JOHN B. SHADEGG, Arizona
STEVEN C. LaTOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
JOHN E. SUNUNU, New Hampshire
PETE SESSIONS, Texas
MICHAEL PAPPAS, New Jersey
VINCE SNOWBARGER, Kansas
BOB BARR, Georgia
DAN MILLER, Florida
RON LEWIS, Kentucky

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
GARY A. CONDIT, California
CAROLYN B. MALONEY, New York
THOMAS M. BARRETT, Wisconsin
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JUDITH McCOY, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

PETE SESSIONS, Texas
THOMAS M. DAVIS, Virginia
JOE SCARBOROUGH, Florida
MARSHALL "MARK" SANFORD, South Carolina
JOHN E. SUNUNU, New Hampshire

DENNIS J. KUCINICH, Ohio
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
CAROLYN B. MALONEY, New York
JIM TURNER, Texas

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
JOHN HYNES, *Professional Staff Member*
MATTHEW EBERT, *Clerk*
KAREN LIGHTFOOT, *Minority Professional Staff Member*

CONTENTS

PROTECTING HEALTH INFORMATION: LEGISLATIVE OPTIONS FOR MEDICAL PRIVACY

TUESDAY, MAY 19, 1998

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 311, Cannon House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Davis, Kucinich, and Maloney.

Staff present: J. Russell George, staff director and chief counsel; John Hynes, professional staff member; Matthew Ebert, clerk; and Karen Lightfoot, minority professional staff member.

Mr. HORN. A quorum being present, the Subcommittee on Government Management, Information, and Technology will come to order.

Today, we continue our consideration of the best way to protect medical privacy. This issue has received a great deal of attention lately. There seems to be a growing feeling among the American public that in our high-tech, fast-moving economy, privacy is now more vulnerable than ever before. I think this feeling is a very accurate one.

The question for Congress, of course, is what to do about the problem. This means beginning with a careful definition of it. Although the debate over medical privacy solutions has been underway for some time now, it is useful to remind ourselves of the problem we're trying to fix. What breaches of confidentiality are currently taking place and would be addressed by the kind of legislation we're discussing? In this connection, we should be clear with exactly how far we can go in solving the problem simply by removing a patient's identity in the medical records and replacing it with some kind of coded identifier.

With the problem carefully defined, we're interested in discussing the specific challenges that arise in trying to protect health information through Federal law. Perhaps the first challenge is the degree to which a Federal law protecting medical privacy should rely on the patient's consent for disclosure of their medical information. Congress must choose whether to define by law the appropriate uses for health information or whether, at least, to a certain extent this definition can be left to negotiations between the provider and the patient. Some level of patient consent seems essential. At the same time, the consent must be meaningful. Do patients really

have any say in the consent forms they must sign in order to receive treatment? This is a very important question, and we will focus on that today.

A second challenge is the preemption issue. Should a Federal law protecting medical privacy preempt all State laws in the same area? Should it preempt only those that are weaker? Should exceptions to preemption be made for mental health laws? These are extremely difficult questions. We would like to hear about what progress has been made, or perhaps, could be made on finding solutions that work.

A third challenge is how to treat research. What kind of access should researchers have to medical records? On this question we need to be very clear about when researchers need the patients' identities and when they do not. We also need to be clear about when researchers need to be able to access the patient's identities even though those identities have been removed from the records. We cannot move forward on legislation until we have a better idea of what information researchers need, where they find it, and how they use it.

A fourth challenge is law enforcement access to medical information. What level of access does law enforcement need? In the case of fraud and abuse investigations, do they need medical records that identify the patients? A fifth challenge is whether any types of health information should be granted special treatment. Categories of information, often mentioned for special treatment include genetic and mental health information. There is considerable resistance to this type of segregation of medical records, but we want to hear from both sides of the issue and see if there is some common ground.

I've listed a broad array of issues. They are all fundamental, they are all complex, and they're all very important. We have highly talented and knowledgeable witnesses who will help us address these issues in some depth. But there's only so much we can cover in one hearing, and some of these challenges deserve more attention than we'll be able to give them today. The Subcommittee on Government Management, Information, and Technology plans to hold focused hearings on the specific challenges of medical privacy legislation in the coming months. As most of you know, the Kassenbaum-Kennedy Act established a deadline of August 1999 for enactment of medical privacy legislation. If Congress does not meet this deadline, the Secretary of Health and Human Services will promulgate regulations. We can all agree that this issue is too important for Congress to leave to the regulators without full debate and congressional direction. But the clock is ticking. There will be very little time for deliberation between January and August of next year as the new Congress finds its footing on all sorts of issues. We're interested in the witnesses' thoughts on this timeframe and on what needs to be accomplished this year.

I'm now delighted to yield to the ranking minority member on the subcommittee, Mr. Kucinich of Ohio for an opening statement.

Mr. KUCINICH. Thank you very much, Chairman Horn. I applaud you for convening this hearing to discuss the important issue of confidentiality of medical records. I'd also like to commend our colleagues, Representative Shays and Representative Condit, for their

leadership in proposing legislation to deal with this pressing issue, and I want to certainly thank Mr. Shays for being here today.

Health care information is perhaps the most intimate, personal, and sensitive information maintained about an individual. Yet, there is no Federal protection for medical records. Our current system places the burden on States and little uniformity exists in the State's laws. This uneven patchwork is increasingly insufficient in today's highly complex health care system, where more and more information is electronically stored and transmitted to multiple individuals and entities across State lines for a multitude of purposes.

Today's medical record contains vast amounts of personal information, not only about diagnosis and treatment, but also about employment history, financial history, and lifestyle choices. As this information contained in medical records grows, Americans are becoming increasingly concerned that this information be adequately protected. This is particularly true as reports of misuse of individuals' health information continue to surface.

Earlier this year, the large drug chain, CVS and Giant Food, admitted to disclosing patient prescription records to a pharmaceutical company, so it could track and market to customers who do not refill prescriptions. A Boston-based HMO admitted they maintained detailed notes from psychotherapy sessions and computer records that were accessible by all clinical employees. A University of Illinois study found that one-third of Fortune 500 companies review private health information before hiring workers.

Misuse and the potential for misuse of confidential medical information is staggering, particularly as data bases are merged without individuals having any idea of who's got their hands on personal, private information.

I have brought detailed testimony here which I'm going to give to the Chair with his generosity of including it in the record.

Mr. Chairman, I have the dubious distinction today of being a ranking member on two subcommittees. A hearing also is taking place on the Kyoto Protocols which I'm going to have to go to to make an opening statement on. I hope to have a chance to return soon, and I certainly know that this committee is in excellent hands.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

Statement of the Honorable Dennis Kucinich
GMIT Subcommittee: Protecting Health Information
May 19, 1998

Mr. Chairman, I applaud you for convening this hearing to discuss the important issue of confidentiality of medical records. I also commend Representative Shays and Representative Condit for their leadership in proposing legislation to deal with this pressing issue.

Health care information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual. Yet there is no federal protection for medical records. Our current system places the burden on states, and little uniformity exists in the states' laws. This uneven patchwork is increasingly insufficient in today's highly complex health care system, where more and more information is electronically stored and transmitted to multiple individuals and entities across state lines for a multitude of purposes.

Today's medical record contains vast amounts of personal information -- not only about diagnoses and treatment - but also about employment history, financial history, and lifestyle choices. As this information contained in medical records grows, Americans are becoming increasingly concerned that this information be adequately protected. This is particularly true as reports of misuse of individuals' health information continue to surface.

Earlier this year CVS and Giant Food admitted to disclosing patient prescription records to a pharmaceutical company so it could track and market to customers who don't refill prescriptions. A Boston-based HMO admitted they maintained detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. And a University of Illinois study found that a third of Fortune 500 companies review private health information before hiring workers. The misuse -- and potential for misuse -- of the confidential medical information is staggering.

In order for our health care system to function, we must ensure the privacy of patients' medical records. Patients must be confident that the sensitive information they share with their physicians will be treated with the strictest respect. Only if patients are willing to share sensitive information with health care professionals, can our health care system continue to provide the best care.

But I also recognize that many others in the health care system may have a legitimate need for information contained in medical records. The data may be need by doctors, researchers, and others working to enhance the quality of health care, to control costs, and to protect the public health.

The challenge facing us is how to address these needs while respecting an individual's right to privacy. It is clear that the traditional methods of managing and regulating medical information are no longer adequate. We need to find a new paradigm which will recognize the complexities of the modern health care system, computer technology, and individual privacy rights.

I am pleased to welcome my colleagues here today to talk about their proposals and to welcome the witnesses representing health care providers, payers, and consumers. I look forward to learning about the new proposal being put forth today and to gaining a better understanding of how this legislation will impact patients, providers, and others involved in health care.

Mr. HORN. We thank you for that thought, Dennis, and it will certainly be put in the record as read.

I now yield to the gentleman from Virginia, Mr. Davis.

Mr. DAVIS. Thank you and I'll be brief, Mr. Chairman.

I agree with you that privacy is more vulnerable now than ever before. This growing technology enables us to get information correlated, and put together and exchanged over the Internet and other mediums. Also, if Congress doesn't resolve this issue by next August, Secretary Shalala will be required under current law to issue regulations. That, of course, can be extended, but barring something like that happening, I think we owe this a very strong oversight at this point to decide what our next move should be.

Many of the solutions that are being proposed, expose druggist small businesses to a mountain of additional paperwork which takes their eye off their core missions, issuing prescriptions and providing quality medical care to people. You have to find adequate balance as we work through this.

I was viewing a Washington Post editorial of February 18, 1998—and this goes to the issue of just a lot of misinformation that goes on this issue. The Post talks in their editorial—big print, big headline:

> Does the average person mind when after having a prescription filled at the pharmacist, he or she starts getting related junk-mail from drug companies to which the pharmacy has passed along his or her name, address, and medical condition?

And it goes on to say "anyone who finds this a difficult question ought to glean a big broad hand at the answer from the fierce consumer reaction." And then they say, "that several local pharmacies including Giant Foods and CVS have entered into such arrangements with a Massachusetts-based company, Elensys."

The problem with that is, in fact, they hadn't done that at all, and of course, the next day, in much smaller print somewhere in an obscure place in the paper, it notes:

> In the editorial yesterday, it incorrectly stated that several large pharmacies including Giant and CVS passed along to drug companies the names of persons having prescriptions filled at the pharmacy, and in fact, that did not happen.

So I think getting to the facts is very, very important in this, and there seem to be a lot of agendas out there as we work our way through this. But this is a very serious matter.

I congratulate the chairman on holding this hearing and others, and I'm sure we'll be exposed to a wide variety of views as we move through and try to understand and do what is right. Thank you.

I ask the committee's consent that the editorial and the accompanying correction be made a part of the record.

[The information referred to follows:]

The Washington Post

Sunday, February 15, 1998

Prescription Sales, Privacy Fears

CVS, Giant Share Customer Records With Drug Marketing Firm

Robert O'Harrow Jr.
Washington Post Staff Writer

Using technology in a new way to market drugs, CVS Corp. and Giant Food Inc. are sending confidential prescription information to a Massachusetts company that tracks customers who don't refill prescriptions, a practice that some experts say raises new questions about medical privacy.

The company, a computer database marketing specialist, uses the data to send personalized letters -- written on pharmacy letterhead and sometimes paid for by drug manufacturers -- that either remind customers to keep taking their medicine or pitch new products that will treat the customer's ailment.

"Our records indicate that you have tried to stop smoking using a prescription nicotine replacement product," said one such letter, recently received by a customer, touting a new drug called ZYBAN. "We hope you successfully quit smoking but if you, like many others who have tried to quit, are still smoking, we have good news for you."

The letter was signed, "Your CVS Pharmacists." In fine print, the letter noted that its mailing was "supported" by Glaxo Wellcome Inc., the maker of ZYBAN. It also said that "no information about you or your prescription has been provided to Glaxo Wellcome."

The chains' stores are among thousands of local pharmacies across the nation that electronically provide names, medication and other personal information to Elensys Inc., a Woburn, Mass., company. Elensys both manages the pharmacies' data and arranges for drug manufacturers to pay pharmacies for the right to send "educational material" to customers with particular ailments and conditions.

Giant and CVS officials said their efforts will help customers stay healthy. But regulators and privacy specialists said the initiatives raise questions about patient confidentiality and blur the line between medicine and marketing.

"It's a gross invasion," said George D. Lundberg, a physician and editor of the Journal of the American Medical Association, who called the practice a "breach of fundamental medical ethical issues."

"Do you want . . . the great computer in the sky to have a computer list of every drug you take, from which can be deduced your likely diseases -- and all without your permission?" Lundberg asked.

Pharmacy regulators in Virginia, Maryland and elsewhere say the practice also may violate confidentiality rules governing the release of medical information. Safeway Inc. officials backed away from plans to sign on with Elensys after Maryland authorities expressed such concerns several times last year. Last month, Virginia legislators introduced bills that would expand prohibitions against the release of prescription data by pharmacists or pharmacy owners.

"The public needs to be very much aware. It's something at the federal level our government needs to address very quickly," said Franklin Z. Wickham, president of the National Association of Boards of Pharmacy, a group of state regulatory agencies. "There's a real potential for abuse."

Giant and CVS officials defended their programs, saying customers benefit from their reminders and from the information provided by drug manufacturers. Both companies said they value customer privacy and allow customers to remove themselves from participation by submitting an "opt-out" form. The ZYBAN letter, for instance, included an attachment that the customer could fill out and send back to CVS, stating, "I do not wish to receive any prescription-related mailings from CVS/pharmacy."

"We are very aware of the confidentiality issue," said CVS spokesman Frederick McGrail, adding that the company does not give Elensys everything in its files about customers. "It's important to us the confidentiality of that information, and the integrity of the patient's information, is maintained. And it is in this case."

Russell Fair, Giant's vice president of pharmacy operations, said his company will make more money and its customers will be healthier under the program. "It's a real win-win situation," Fair said.

Elensys's president, Daniel E. Rubin, said drug companies never get access to the pharmacy's files. When a pharmaceutical company wants to contact people with particular ailments, it pays the pharmacy and Elensys to mail out its materials. He said Elensys is not violating state confidentiality prohibitions because it acts as an agent -- not an outside party -- for the pharmacies that send it information.

"We basically process their data," Rubin said. "It's basically still within the chain, in fact, because we're an agent for the chain."

The efforts underway at CVS, the area's largest drugstore chain, and Giant, which is the largest grocery retailer in the area and is opening free-standing drugstores, are called "drug compliance programs."

They are part of a far-reaching move by drug manufacturers and pharmacies across the country to make greater use of medical information, new technology and sophisticated marketing techniques to sell more drugs. Rather than promoting their wares mainly to doctors, the companies are increasingly going directly to patients, hoping they will ask their doctors to prescribe a specific medication.

One technique now used by drug advertisers and manufacturers is to automatically capture and store personal data about the people who call toll-free phone numbers seeking information about such medications as Claritin, an antihistamine, and Valtrek, a herpes treatment. These initiatives got a boost last August when the Food and Drug Administration loosened some restrictions on the television advertising of drugs if drug companies included a toll-free number that customers can call for more information.

Meanwhile, RxRemedy magazine has created a database of health information with about 2.2 million subscribers, 55 and older, who responded to offers to receive the publication free in exchange for filling out a medical survey. That database is used by pharmaceutical companies and others to analyze drug-taking behavior and market new products directly to consumers.

Pharmaceutical manufacturers sold about $80 billion in brand-name and generic prescription drugs last year, according to Pharmaceutical Research and Manufacturers of America, a trade organization.

Drug companies spent almost $875 million last year on television, newspaper and other consumer advertising, more than five times the $164 million they spent in 1993, according to Scott-Levin, a health care consulting company.

Rite Aid Corp., the second-biggest drugstore chain in the Washington area, has developed its own database operation that also uses computers to find customers who have not refilled prescriptions. After the company identifies particular customers, telephone operators call them at home to urge them to follow their doctor's instructions, according to Suzanne Mead, a Rite Aid spokeswoman.

All these efforts are driven by innovations in computers and other technology that allow analysts to draw finer distinctions from vast repositories of medical and prescription information than ever before, according to Lynn O'Connor Vos, chief executive for Grey Healthcare Group, a marketing company.

A key aim is to directly contact customers with specific ailments, and then to persuade them to ask their doctors to prescribe certain drugs, Vos said.

"You've got to reach your customers psychologically and emotionally," Vos said. "There's going to be an explosion of opportunity in the pharmaceutical industry for database marketing."

Vos and others marketing specialists cite Elensys, whose name is a variation on the name of an ancient Greek city known for medicine and health, as a leader of the trend. The company started operations with a handful of people almost five years ago. In 1995, it began analyzing prescription data from fewer than 500 pharmacies and, under the auspices of local stores, started mailing letters to several thousand customers.

Today, Elensys receives prescription information from 15,000 pharmacies about millions of people every week, and it uses some of the most sophisticated computer equipment available to keep track of the records, according to Elensys's Rubin. In a posting on the Internet, Elensys describes itself as "the leader in patient behavior modification programs."

Interest in the company has soared, in part because so many people fail to take medicine properly and most chains don't have the technical wherewithal to track customers as precisely as Elensys, Rubin said. Up to half of all patients who should routinely take medicine for such ailments as hypertension or high cholesterol quit prematurely, he said. "It's the primary reason for our existence."

Much of the cost of the analysis and mailings is offset by payments from drug manufacturers, who contract with pharmacies for the right to mail information to individual customers. Among other things, Rubin said, that material could include suggestions that customers switch from one drug to another.

CVS signed on with Elensys in September to track customers who take a heart medication called Posicore, and the company intends to expand mailings in the near future, McGrail said. Giant began sending the customer data late last year and recently used Elensys to identify customers with hay fever for a marketing campaign, Fair said.

Some state officials are questioning the arrangements, however. After Safeway expressed interest in signing on with Elensys last year, the Maryland Board of Pharmacy questioned whether the program would violate regulations protecting patient confidentiality, according to several board letters and the minutes of meetings.

Maryland law generally prohibits release of medical records, including prescription information, without patient authorization. That means drugstores or chains that release

information to a third party may be in violation of state regulations, according to David M. Russo, president of the board.

"That's a breach of confidence, according to the state board," Russo said, adding that Giant and CVS have not approached the board for an opinion.

CVS's McGrail said "the goal behind these [programs] is to improve care. . . . It's not as though we're turning over the entire file to Elensys."

Giant's Fair stressed that Elensys does not share its prescription database with third parties. "They don't have secondary interests," Fair said.

A Safeway spokesman said it backed away from Elensys after the pharmacy board raised concerns. "The reason we're not going forward at this time is our concern with patient confidentiality," said Gregory TenEyck, a Safeway spokesman. "The relationship is between Safeway and the customer. Anyone entering into that is a concern to Safeway."

In Virginia, pharmacy regulators were not aware of the drug compliance programs at CVS and Giant. But soon after The Washington Post asked questions about Elensys, the Board of Pharmacy began exploring whether those programs violated any state regulations, according to executive director Elizabeth Scott Russell.

"We are looking into whether there is activity in violation of our confidentiality rules," she said.

Russell said she wanted to see whether customers had signed explicit waivers before their prescription and personal information was sent to Elensys. With few exceptions "it would be a violation of a Board of Pharmacy rule for a pharmacy to disclose any medical information," Russell said.

Virginia Sen. Joseph Gartlan Jr., who has introduced legislation that would strengthen rules prohibiting pharmacists from releasing prescription data, said he acted after his pharmacist discovered that patient information had made its way to drug companies through other means. "What's at stake is my privacy and, in the extreme case, my health," Gartlan said.

Medical ethics specialists also questioned the propriety of drug compliance programs. Robert Veatch, a professor of medical ethics at the Kennedy Institute of Ethics at Georgetown University, said such efforts could have a very positive effect by encouraging patients to take their medicine. But he worries that they also diminish the barrier between medicine and marketing.

"The essence of the problem is you have an entrepreneurial ethic, where the goal is to sell the product, in direct conflict with the more traditional medical ethic, where the goal is the well-being of the patient," Veatch said. "It seems to me that conflict is so basic it's probably indefensible."

But Rubin said his company's services maintains that line, while giving drug companies and local pharmacies an opportunity to make more money.

"This is good medical and good entrepreneurial" practice, Rubin said, "which is the nice thing about it."

Washington Post
February 18, 1998

Correction

An editorial yesterday incorrectly stated that several large pharmacies, including Giant and CVS, passed along to drug companies the names of persons having prescriptions filled at the pharmacy. In fact, Giant and CVS sent data to a marketing company to track and write to pharmacy customers who had not yet re-filled prescriptions, but that company was under contract not to release the personal data to drug companies or others.

Washington Post February 18, 1998

When Private Means Private

DOES THE AVERAGE person mind when, after having a prescription filled at the pharmacist, he or she starts getting related junk mail from drug companies to which the pharmacy has passed along his or her name, address and medical condition? Are such customers likely to be pleased at the convenience—as the pioneers of this new form of medical marketing insist they ought to be—or are they likelier to bristle at the implied violation of their privacy? Anyone who finds this a difficult question ought to glean a big, broad hint at the answer from the fierce consumer reaction to a report in this newspaper Sunday that several large area pharmacies, including those at the Giant Food Inc. and CVS chains, have entered into such arrangements with a Massachusetts-based company called Elensys. Today, in full-page ads and other formats, Giant announces it will stop providing such information—reacting to what spokespeople said had been a flood of calls from angry consumers.

And what were pharmacists—next door to doctors in their access to privileged, personal knowledge about people's ailments—doing marketing such information in the first place? The answer casts some light on the strange tensions being set up everywhere by the financial possibilities—one might better call them temptations—of the so-called "information economy," in which information about one's customers and their needs has become a vast new resource to be mined. It shouldn't surprise anyone that consumers feel more strongly about their medical prescriptions than they do about the great amounts of other information now routinely collected from every financial transaction, whether it's traveling, shopping or browsing the Internet. But information about people's preferences—meaning the sorts of things they are likely to do, or read or buy—is by far the most valuable of the various sorts of information now being briskly harvested and traded on all sides. Any company that collects such information in the ordinary course of business is sitting on a gold mine—and can be expected to act on that fact in the absence of specific, spelled-out public limits.

To what extent should people's needs be allowed to be treated this way, as some sort of naturally occurring resource available to anyone who can grab it? The outcry over drug prescriptions suggests one such limit. While some forms of sensitive information, such as credit information, are now protected, the sheer variety of types of medical data have made progress slow on protecting them.

Prescription information falls near the line between purely medical data and commercial information, but as the reaction makes clear, that line has been crossed. Besides being inherently more sensitive and personal than information about shopping choices, prescriptions are also in a real sense less optional: Nobody "chooses" to have a particular ailment or to release the information about that ailment into the wider data stream of junk mail. The arrangements with Elensys, which contracts to manage pharmacists' data about patients and to make selected bits of it available so drug companies can send potential patients "educational material" about their inferred ailments, are just ingenious enough to focus people's attention on where they want that line drawn.

2-19-98

Correction

An editorial yesterday incorrectly stated that several large pharmacies, including Giant and CVS, passed along to drug companies the names of persons having prescriptions filled at the pharmacy. In fact, Giant and CVS sent data to a marketing company to track and write to pharmacy customers who had not re-filled prescriptions, but that company was under contract not to release the personal data to drug companies or others.

Mr. HORN. Without objection, they are a part of the record at this point.

We're now delighted to introduce our first witness, a very distinguished colleague in this body, highly respected by people on both sides of the aisle, the gentleman from Connecticut, Mr. Christopher Shays. Welcome.

STATEMENT OF HON. CHRISTOPHER SHAYS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CONNECTICUT, ACCOMPANIED BY JOEL WHITE, PROFESSIONAL STAFF MEMBER

Mr. SHAYS. Thank you, Chairman Horn. I'm joined by a member of my staff, Joel White, who literally spent 2 years working on the legislation that I'll be talking about today. I'm going to ask the chairman's indulgence—in the 11 years that I've been here, I think I've read a statement to a committee, one other time—but, I'd like to read my statement because it's fairly comprehensive, and I don't want to leave certain parts out, with your indulgence.

Mr. HORN. Please do.

Mr. SHAYS. Thank you.

Mr. Chairman and Congressman Davis, thanks for the opportunity to provide you with my thoughts on medical records confidentiality and the bill that I will be introducing today with Congressman Tom Barrett.

When I began looking into this issue more than 2 years ago, I was not prepared for the degree of complexity and the competing interests involved in one of the most important issues Congress will address over the next 2 years.

I am happy we are introducing the Consumer Health and Research Technology [CHART] Protection Act. We believe this bill is a strong step forward in protecting sensitive health information. In addition, I am also pleased that on May 14, at New York University, Vice President Gore announced the administration's support for passing legislation this year to protect medical record's confidentiality. I look forward to working with the Vice President and with other Members of Congress to enact a comprehensive bill.

Mr. Chairman, this issue has no easy answers. The bill we are introducing today is a work-in-progress. We are open to suggestions, improvements for changes to enhance confidentiality safeguards.

In my view, there are three main areas of controversy surrounding the protection of medical information. One, authorization for use of individually identifiable health information; two, preemption of State law; and three, the right to inspect, copy, and amend one's own individual record. While the issues involved are complex, I'd like to highlight the challenges involved in addressing all three, and what the CHART Protection Act does in each area.

Under authorization for use of individually identifiable health information, the CHART Protection Act will safeguard the confidentiality of medical records while protecting legitimate uses. The legislation delineates the inappropriate uses of medical information such as: Intentional or negligent disclosure; sale or commercial publication; or, the use of fraud, deceit, or misrepresentation to access information. These prohibitions relate specifically to individ-

ually identifiable information. Use of anonymous information will not be affected, unless it's intentionally decoded.

This is an important departure from the approach contemplated in S. 1921, the Health Care PIN Act, introduced by Senator Jeffords, or S. 1368, the Medical Information, Privacy, and Security Act, introduced by Senator Leahy, or Senator Bennett's draft proposal. Those bills seek to restrict the use of health information, unless specifically authorized for a disclosure. In some instances, it may be necessary to obtain a patient's authorization during the same hospital stay for the same admission because disclosable events could trigger an authorization to use individual health information for treatment, payment, and quality activities. While I can understand the concerns of some, that in every instance an individual should affirmatively authorize disclosure of protected health information. I'm concerned Congress would contemplate making the delivery of health services so burdensome to quality improvement, a utilization review could be impossible. We want to make sure managed care organizations, for instance, have access to information they need to conduct quality management activities that directly improve the care our constituents receive.

The CHART Protection Act escapes much of this controversy by creating a single-tiered authorization for use of individually identifiable health information by providing the authorization up-front, but it allows individuals the option to revoke their authorization at any time for health research purposes.

Most of the Senate proposals create a two-tiered authorization process in which treatment, billing, and health care operations are in the first tier, while all other uses are subject to separate authorization including use of information for research purposes. This has been the source of much controversy. For example, any individual who withholds their authorization for research purposes, can skew the outcomes of an entire health study. Ultimately, this damages our ability to enhance medical knowledge and improve patient care dealing with preemption of State law.

The CHART Protection Act generally preempts State law except mental health and communicable disease protections enacted by States and localities, as well as public health law, such as birth and death reporting. Some believe this approach hinders important privacy advances already enacted by some communities. Others believe the bill doesn't go far enough, that all health information should be preempted so there is only one uniform Federal standard.

I believe the answer lies somewhere in between. Those who argue the former, believe States should be allowed to enact more stringent privacy standards. They believe Federal law should set a floor, not a ceiling. They ignore, however, recent and not-so-recent advances in how we pay for and deliver health care. Computers are increasingly blurring State lines with respect to where information is kept, stored or sent. Multi-State health plans that submit bills to clearing houses, who then forward claims to separate payers, cannot operate through a maze of differing standards, regulations, and restrictions.

In addition, with strong Federal legislation that creates workable confidentiality standards, State protections would be unnecessary.

I do believe, however, that some localities have enacted very specific protections for certain segments of their population that should be maintained. These are the laws designed to protect our challenged populations: Those with mental illnesses or communicable diseases. Considering these protections go right to public health and safety, local rules should apply.

Finally, the ability to inspect, copy, and amend medical records. The CHART Protection Act allows patients to inspect, copy, and where appropriate, amend their medical records. This is an area where there is large agreement. In fact, all of the proposals introduced in the House and Senate allow patients to inspect, copy and amend their medical records, a right they do not currently enjoy unless they live in 1 of the 28 States that offers this protection.

Some are concerned that allowing individuals to amend their medical records could change the original record, and therefore, the obligations of the health plan are insured. Let me be very clear, the CHART Protection Act in no way would alter the liability of health plans or insurers to pay for health services.

Finally, the CHART Protection Act proposes strong criminal and civil penalties for inappropriate disclosures. Because of the stiff penalties in the bill, I believe many will choose to use medical records that have been deidentified or anonymized. Under our legislation, anonymized information falls outside the scope of the bill creating powerful incentives to anonymize data.

Those who seek to secure absolute privacy in a health context are jeopardizing our ability to effectively deliver health services. We need to balance competing interests between a person's legitimate expectation of confidentiality and a business's need to know what it is paying for.

In my judgment, the way to accomplish this is to leave the computer data bases alone, and criminalize misuse of their data, recognizing that there are both appropriate and inappropriate uses for medical information. With current technology and future advances, there are both real dangers and substantial opportunities with respect to protected health information. Absent strong, practical, and workable standards many will fall victim to those dangers and opportunities will be missed.

Innovative developments in the delivery of health services and technological advancements mean health information is both more important and more vulnerable. While we will all agree, sensitive information, such as psychological evaluations and drug-abuse counseling, needs to be kept private, we also need to allow health plans and researchers to review health information to improve education and treatment.

Under the Health Insurance Portability and Accountability Act known as, HIPAA or Kassebaum-Kennedy, Congress set a schedule for action on this issue. Should Congress fail to enact comprehensive legislation to protect the confidentiality of patient records by August of next year, the Secretary will promulgate regulations by February 2000. I believe Congress should act before the Secretary steps in.

It is my hope that we can pass a national confidentiality law ensuring patients' rights while balancing the interests of payers and providers, data processors, law enforcement agencies, and research-

ers. I agree with Vice President Gore that Congress should pass legislation to secure the confidentiality of medical records, and it should be done this year.

Mr. Chairman, I appreciate the opportunity to testify before your committee, and I also appreciate your indulgence in letting me read a statement. Thank you.

[The prepared statement of Hon. Christopher Shays follows:]

Statement of Congressman Christopher Shays
Before the Subcommittee on Government Management, Information and Technology of the Government Reform and Oversight Committee
May 19, 1998

Thank you Mr. Chairman and Members of the Subcommittee for the opportunity to provide you with my thoughts on medical records confidentiality and the bill that I will be introducing today with Congressman Tom Barrett.

When I began looking into this issue more than two years ago, I was not prepared for the degree of complexity and the competing interests involved in one of the most important issues Congress will address over the next two years. I am happy we are introducing the Consumer Health And Research Technology (CHART) Protection Act. We believe this bill is a strong step forward in protecting sensitive health information.

In addition, I am also pleased that on May 14 at New York University, Vice President Gore announced the Administration's support for passing legislation this year to protect medical records confidentiality. I look forward to working with him, and others in Congress to enact a comprehensive bill.

Mr Chairman, this issue has no easy answers. The bill we are introducing today is a work in progress. We are open to suggested improvements or changes to enhance confidentiality safeguards.

In my view there are three main areas of controversy surrounding the protection of medical information:

authorization for use of individually identifiable health information;

preemption of state law;

and the right to inspect, copy and amend one's own individual records.

While the issues involved are complex, I'd like to highlight the challenges involved in addressing all three and what the CHART Protection Act does in each area.

1.) Authorization for use of individually identifiable health information. The CHART Protection Act will safeguard the confidentiality of medical records while protecting legitimate uses. The legislation delineates the inappropriate uses of medical information -- such as intentional or negligent disclosure, sale or commercial publication, or the use of fraud, deceit or misrepresentation to access information. These prohibitions relate specifically to individually identifiable information. Use of anonymous information will not be affected, unless intentionally decoded.

This is an important departure from the approach contemplated in S. 1921, the Health Care PIN Act introduced by Senator Jeffords, or S. 1368, the Medical Information Privacy and Security Act introduced by Senator Leahy, or Senator Bennett's draft proposal. Those bills seek to restrict the use of health information unless specifically authorized for a disclosure.

In some instances, it may be necessary to obtain a patient's authorization during the same hospital stay for the same admission because each disclosable event could trigger an authorization to use individual health information for treatment, payment and quality activities.

While I can understand the concerns of some that in every instance an individual should affirmatively authorize disclosure of protected health information, I'm concerned Congress would contemplate making the delivery of health services so burdensome that quality improvement or utilization review could be impossible.

We want to make sure managed care organizations have access to information they need to conduct quality management activities that directly improve the care our constituents receive.

The CHART Protection Act escapes much of this controversy by creating a single-tiered authorization for use of individually identifiable health information by providing the authorization up front, but allows individuals the option to revoke their authorization at any time for health research purposes.

Most of the Senate proposals create a two tiered authorization process in which treatment, billing and "health care operations" are in the first tier, while all other uses are subject to a separate authorization, including use of information for research purposes. This has been the source of much controversy. For example, an individual who withholds their authorization for research purposes can skew the

outcomes of an entire health study. Ultimately this damages our ability to enhance medical knowledge and improve patient care.

2.) Preemption of state law. The CHART Protection Act generally preempts state law except mental health and communicable disease protections enacted by states and localities, as well as public health laws such as birth and death reporting. Some believe this approach hinders important privacy advances already enacted by some communities. Others believe the bill doesn't go far enough; that all health information laws should be preempted so there is only one uniform, federal standard. I believe the answer lies somewhere in between.

Those who argue the former believe states should be allowed to enact more stringent privacy standards. They believe federal law should set a floor not a ceiling. They ignore, however recent, and not so recent, advances in how we pay for and deliver health care.

Computers are increasingly blurring state lines with respect to where information is kept, stored or sent. Multi-state health plans that submit bills to clearinghouses who then forward claims to separate payors cannot operate through a maze of differing standards, regulations and restrictions. In addition, with strong federal legislation that create workable confidentiality standards, state protections would be unnecessary.

I do believe, however, that some localities have enacted very specific protections for certain segments of their population that should be maintained. These are the laws designed to protect our challenged populations: those with mental illness or communicable diseases. Considering these protections go right to public health and safety, local rules should apply.

3.) Ability to inspect, copy and amend medical records. The CHART Protection Act allows patients to inspect, copy and, where appropriate, amend their medical records. This is an area where there is large agreement. In fact, all of the proposals introduced in the House and Senate allow patients to inspect, copy and amend their medical records, a right they do not currently enjoy unless they live in one of the 28 states that offers this protection. Some are concerned that allowing individuals to amend their medical records could change the original record and therefore, the obligations of a health plan or insurer. Let me be very clear: The CHART Protection Act in no way would alter the liability of health plans or insurers to pay for health services.

Finally, the CHART Protection Act imposes strong criminal and civil penalties for inappropriate disclosures. Because of the stiff penalties in the bill, I believe many will choose to use medical records that have been de-identified, or anonymized. Under our legislation anonymized information falls outside the scope of the bill, creating powerful incentives to anonymize data.

Those who seek to secure absolute privacy in a health context are jeopardizing our ability to effectively delivery health services. We need to balance competing interests, between a person's legitimate expectation of confidentiality and a business's need to know what it is paying for. In my judgment, the way to accomplish this is to leave the computer databases alone -- and criminalize misuse of their data, recognizing there are both appropriate and inappropriate uses for medical information.

With current technology and future advances there are both real dangers and substantial opportunities with respect to protected health information. Absent strong, practical and workable standards, many will fall victim to those dangers and opportunities will be missed.

Innovative developments in the delivery of health services and technological advancements mean health information is both more important and more vulnerable. While we can all agree sensitive information such as psychological evaluations and drug abuse counseling needs to be kept private, we also need to allow health plans and researchers to review health information to improve education and treatment.

Under the Health Insurance Portability and Accountability Act, known as HIPAA or Kassebaum-Kennedy, Congress set a schedule for action on this issue. Should Congress fail to enact comprehensive legislation to protect the confidentiality of patients' medical records by August of next year, the Secretary will promulgate regulations by February 2000. I believe Congress should act before the Secretary steps in.

It is my hope we can pass a national confidentiality law assuring patients' rights, while balancing the interests of payors and providers, data processors, law enforcement agencies, and researchers. I agree with Vice President Gore that Congress should pass legislation to secure the confidentiality of medical records, and it should be done this year.

Mr. Chairman, I appreciate the opportunity to share these views with you and am happy to answer any questions you may have.

Mr. HORN. I thank the gentleman.

Does the gentleman from Virginia have any questions of the witness?

Mr. DAVIS. No, Mr. Chairman.

Mr. HORN. OK, let me ask one question that comes to mind. Your bill takes a fundamentally different approach than the other major proposals, in that it doesn't attempt to define permitted uses of health information, it only addresses what is prohibited. Could you explain this approach? Why did you happen to choose it and what advantages does it bring?

Mr. SHAYS. Yes. We have 10 prohibitions. We just felt it was clearer to state why there should be a prohibition. And we also state eight times where it is allowed. So we really are doing both. We want it to be fairly clear and I think we do it without—I think it's less ambiguous.

Mr. HORN. Under your bill, can patients decline to authorize the use of their medical information for particular uses?

Mr. SHAYS. For research only. In fact, what's unique about our bill is they do it up front.

Mr. HORN. Would there be any suffering of consequences from this if they did decline?

Mr. SHAYS. On the research?

Mr. HORN. Yes.

Mr. SHAYS. Well, if they do it up front, then the pool that researchers will use they'll already know what the pool is, instead of having a larger pool and then having someone opt-out.

Mr. HORN. Well, we appreciate all the hard work you've given this and we'll obviously be in touch with you throughout the development of this legislation.

Mr. SHAYS. Mr. Chair, I appreciate the work you put in, and I appreciate that you're taking this up now and not waiting. Thank you very much.

Mr. HORN. Thank you.

With that, we will now move to panel two. I don't believe Mr. Condit is here. We have various information that we'll put in the record on Mr. Condit's legislation.

[The prepared statement of Hon. Gary A. Condit follows:]

COMMITTEE ON AGRICULTURE
SUBCOMMITTEE ON RISK MANAGEMENT AND SPECIALTY CROPS
RANKING MINORITY MEMBER
SUBCOMMITTEE ON LIVESTOCK, DAIRY AND POULTRY

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
SUBCOMMITTEE ON ECONOMIC GROWTH, NATURAL RESOURCES, AND REGULATORY AFFAIRS
SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL AFFAIRS, AND CRIMINAL JUSTICE

GARY A. CONDIT
18TH DISTRICT, CALIFORNIA

Congress of the United States
House of Representatives

2245 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-0518
(202) 225-6131

DISTRICT OFFICES
FEDERAL BUILDING
855 WEST BEN STREET
MERCED, CA 95340
(209) 383-4455

470 16TH STREET
MODESTO, CA 95354
(209) 527-1914

1800 166-4424
email: Rep.Condit@mail.house.gov

THE HONORABLE GARY A. CONDIT
ON BEHALF OF
HR 52, THE FAIR HEALTH INFORMATION PRACTICES ACT

I want to thank Mr. Horn for his continued interest and support in this area. I am pleased this subcommittee is taking the time and thought needed to address the complex issue of health privacy. As you know, I have introduced HR 52, the Fair Health Information Practices. The purpose of this bill is to establish a code of fair information practices for health information that originates in or becomes a part of the health treatment or payment system.

We all know that health information is not confidential. We have all heard the horror stories:

- Medical students selling names of patients with particular conditions to drug companies
- Bank presidents who serve on health boards calling up the names of people in his bank who have cancer and revoking their loans.
- People afraid of their private medical information being disseminated on the world wide web, do not divulge full disclosure to their doctor about their condition.

For all intent and purpose, the Hippocratic oath is defunct. Confidences are collected and stored in a centralized database for use when you switch insurers, jobs, or apply for life or disability insurance. Our medical histories are now a tool used to decide if you're too sick to be employed or insured.

The need for uniform federal health confidentiality legislation is clear. State laws vary significantly in scope and federal laws are applicable only to limited kinds of information or to information maintained only by the federal government. In a society where patients, providers, and records routinely cross state boarders, it is rarely worth anyone's time to attempt to learn the rules of any one jurisdiction, let alone several jurisdictions. Common rules and common language will facilitate broader understanding and better protection.

My bill would:

- establish uniform, comprehensive federal rules governing the use and disclosure of identifiable health information about individuals.

- specifies the responsibilities of those who collect, use, and maintain health information about individuals
- define the rights of individuals with respect to health information
- provides mechanisms that will allow individuals to enforce their rights.

Protected health information is defined in the bill to include individually identifiable data related to the provision of health care, or the payment for health care. In essence, information is covered if it is created during or becomes part of the treatment or payment process. Health information becomes protected health information when it is created by or is in the possession of a health information trustee.

A health information trustee is someone who uses or maintains protected health information. Health care providers, benefit plans and carriers, oversight agencies, an public health authorities are health information trustees. Others who obtain protected health information infrequently such as health researchers and law enforcement agencies are also health information trustees.

The responsibilities and authorities for each trustee have been carefully defined to balance each individual's right to privacy and the need for confidentiality in the health treatment process against legitimate societal needs such as public health, health research, cost containment, and law enforcement.

Trustees are required to –

- limit disclosure of protected health information to the minimum necessary to accomplish the purpose
- use protected health information only for a purpose that is compatible with and directly related to the purpose for which the information was collected or obtained by the trustee
- maintain appropriate administrative, technical, and physical safeguards to protect integrity and privacy of health information
- disclose protected health information only for an authorized purpose
- maintain an accounting of the date, nature, and purpose of any disclosure of protected health information.

The general rule is that protected health information remains subject to the fair health information practices rules when it is disclosed to a third party. This is a major advance in the protection of health records and fills a significant loophole in most existing confidentiality rules. There are only a few circumstances in which protected health information is disclosed to a third party and does not remain subject to protection. For instance:

- Directory information, i.e., name, location, general condition, may be disclosed if the individual has not objected and if disclosure does not reveal anything about condition or treatment. Directory information is not protected in the hands of the recipients.

- Information may be disclosed to a patient's next of kin if a provider has no reason to believe that the patient would consider the information to be especially sensitive, if the patient has not objected, and if the disclosure is consistent with professional practice. Information disclosed in this manner is not protected in the hands of the recipient.
- Information disclosed by or under the authority of a patient (other than to a health information trustee) is not protected in the hands of the recipient. But limitations agreed to by the recipient are binding and enforceable.

The policy reflected here is that confidentiality duties are not imposed on casual recipients of health information who are not likely to be aware of duties. For example, no one will be subject to a lawsuit for repeating a neighbor has a cold.

A key element of this system is the specification of the rights of patients. Each patient will have a bundle of rights with respect to protected health care information about him or herself that is maintained by a health information trustee. In general, a patient will have the right to inspect and to have a copy of that information. A patient will have the right to seek correction of information that is not timely, accurate, relevant, or complete.

The legislation includes several remedies that will help to enforce the new standards. For those who willfully ignore the rules, there are strong criminal penalties. For patients whose rights have been ignored or violated by others, there are several enforcement mechanisms, including criminal penalties (up to ten years in prison), civil remedies, and civil money penalties that may be imposed by the Secretary of Health and Human Services.

In closing, I want to recognize the limits to this legislation. In today's complex health care environment of third party payers, medical specialization, high cost care, and computerization, it is simply not possible to have complete confidentiality. To elevate each patients privacy interest above every other societal interest would be impractical, unrealistic and expensive. My legislation does not and cannot promise absolute privacy. What it does offer is a code of fair information practices for health information. The promise of that code to professionals and patients alike is that identifiable health information will be fairly treated according to a clear set of rules that protect the confidentiality interests of each patient to the greatest extent possible. While we may not realistically be able to offer any more than this, we surely can do no less for the American public.

As you know there are several other health privacy bills in both the House and Senate. I am encouraged that this subcommittee is taking the time needed and necessary to find a broad consensus on the issue of health privacy. Additionally, I commend the Administration, Vice President Al Gore, and Department of Health and Human Services Secretary, the Honorable Donna Shalala, for their contributions and recommendations to

the privacy debate. I look forward to continue working with this subcommittee and my colleagues on this issue. Thank you.

Mr. HORN. Panel two includes Ms. Goldman, Mr. Nielsen, Dr. Korn, Ms. Frawley, Dr. Harding, Mr. Kahn, and Dr. Andrews. So, if you will come forward, we'll begin.

They're in the order in which I raised it, so you might peek at that sign in front of you. Now there's a tradition we have on this subcommittee. It's an investigating subcommittee. All witnesses, if they're going to testify, must take the oath that their testimony is truthful. So, if you will bear with me, stand up, and raise your right hands.

[Witnesses sworn.]

Mr. HORN. The clerk will note that the seven witnesses are affirmed.

And we will begin with Ms. Janlori Goldman, who is director of the Georgetown University Health Privacy Project.

STATEMENTS OF JANLORI GOLDMAN, DIRECTOR, GEORGETOWN UNIVERSITY HEALTH PRIVACY PROJECT; JOHN T. NIELSEN, SENIOR COUNSEL AND DIRECTOR OF GOVERNMENTAL RELATIONS, INTERMOUNTAIN HEALTH CARE, INC., ON BEHALF OF AMERICAN HOSPITAL ASSOCIATION; DR. DAVID KORN, SENIOR VICE PRESIDENT FOR BIOMEDICAL AND HEALTH SCIENCE RESEARCH, ASSOCIATION OF AMERICAN MEDICAL COLLEGES; KATHLEEN A. FRAWLEY, VICE PRESIDENT, LEGISLATIVE AND PUBLIC POLICY SERVICES, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION; DR. RICHARD HARDING, MEDICAL DIRECTOR, PSYCHIATRIC SERVICES, RICHLAND MEMORIAL HOSPITAL AND VICE PRESIDENT-ELECT, AMERICAN PSYCHIATRIC ASSOCIATION; CHARLES N. KAHN, CHIEF OPERATING OFFICER AND PRESIDENT-DESIGNATE, HEALTH INSURANCE ASSOCIATION OF AMERICA; AND DR. ELIZABETH ANDREWS, DIRECTOR OF WORLDWIDE EPIDEMIOLOGY, GLAXO WELLCOME, INC., ON BEHALF OF PHARMACEUTICAL RESEARCH AND MANUFACTURERS OF AMERICA

Ms. GOLDMAN. Good morning, Mr. Chairman, Congressman Davis.

I appreciate the opportunity to be here this morning not only to testify in front of this subcommittee again on health privacy, but also to commend you for your continued commitment to this issue.

I don't want to suggest that because you've held a number of hearings and worked on this issue for quite a while that we haven't made much progress. I think we have made progress. Certainly, the law that requires passage of legislation by August of next year suggests that we may eventually be looking at passage of legislation.

Last year, I started a project on health privacy at Georgetown University specifically to accomplish a few goals: To raise the public awareness about the need for protection of personal medical information and to work toward common ground as we approach the deadline set by Congress. Many of us here at this table have been working for many years together to achieve that common ground, and I'm hopeful that we'll be able to do it before year's end—certainly by next year.

The project is also focused in a number of other areas. We're putting together a State Compendium of Health Privacy Laws and looking to identify models for best practices in the health care environment.

Protecting people's medical records is not only an important privacy issue as we look at it in a traditional civil liberties context, but it's also a critical health care issue and there's a growing acknowledgment that protecting privacy is important to protecting and improving health care in this country. The President's Commission on Consumer Protection and Quality included confidentiality in its Patients' Bill-of-Rights. It's included in a number of the bills before Congress on Patients' Bill-of-Rights, and as you heard from Congressman Shays, the Vice President also included it as a top priority in a privacy initiative he launched last week.

In looking at privacy we really have two core values: One, which is the traditional value of privacy that we often think of, which is this ability to retreat away from the world, and to seek solitude. But I think the more important value of privacy which we need to address here is the ability for people to step forward and fully participate in society without losing all control over personal information. Particularly here, the price of participation should not be the loss of privacy.

We've seen that heightened public concern about privacy has started to affect behavior in the health care context. And the polling data on this is very strong and very consistent, and I've included some of those numbers in my statement. What we've seen is that there are many factors that are contributing to people's fear as they enter the health care system. Some of it is that changes with managed care have been troubling to people, and we've seen a consolidation of key health care services from providing care, to paying for care, to research and even marketing. The creation of electronic health data networks, while important for public health initiatives has also led people to be more concerned, and we've seen a steady stream of press reports about abuses and misuses of health information.

As Congressman Davis remarked earlier about the CVS and Giant story. Although there may not have been actual disclosures, the public was very concerned about these unexpected and unknown and unconsented to uses of their prescription drug records for other purposes, not directly related to the particular activity. So, out of that public outrage, the companies abandoned those compliance and marketing programs to really sit back and take a better look at this.

What we've seen with those kinds of examples is not necessarily an evil intent. What we've seen is that in an unregulated environment where we don't have enforceable rules, where there is no national standard, everything is fair game. Privacy is not considered a priority in the development of many of these programs, and the consumer voice has been lost.

The changes in the health care system are so rapid that it's very difficult at any point in time just to say, here's where we're going to create a factual record, here's where we're going to look at how to create enforceable rules, because the changes are happening so rapidly. But I think that we need to, in some ways, take a snapshot

of where we are now, and create that factual record and see if we can put some rules in place.

It's important to note, I'd add here, that most of the health care reform initiatives that we talk about, that we push forward, and that we're going to hear about today in terms of outcome analysis and cost-utilization studies on public health and research initiatives, all depend on very high-quality and vast amounts of personal health data. What we need to realize is that information at its source comes from individuals when they talk to their doctors. So, if we want to protect privacy, and also make sure that those public health initiatives move forward, we need to see that these issues are linked.

The National Research Council issued its report last year—for the record—which showed that even though technology is available, which is the good news, to protect privacy and to build security in place, it is not being implemented at a very broad level because there's no real market incentive to do so. There are no real consequences in place. But as I said, the good news is the technology is there to remove identifiers, safeguard information, encrypt data, and put audit trails and access codes in place to guard against unauthorized use.

The mandate to pass legislation by next year should bring us together to achieve consensus. As I said, the individual's health care is at stake because if people don't trust their doctors, they won't share fully, and that information then may be less accurate and incomplete. They'll engage in privacy protective behavior, withhold data, maybe not even seek care. Thus, the downstream use of information for public health and research purposes may also be compromised.

Let me just quickly touch on the key principles that I think most of us have agreed need to be incorporated into legislation, and point out where the current proposals do so.

The good news, again here, is that most of the key principles at the broadest level are incorporated into all of the bills that have been introduced and in the discussion draft before us today; those include people having a right to see their own medical records. All of the bills that have been introduced, all of the discussion drafts including Senator Bennett's proposal and Congressman Shays proposal do include that right. People should be given the ability to know how their information will be used up front so that they can make informed choices. Again, the proposals all incorporate a notice principle.

Where I think there's been some concern is how to deal with informed consent, how to build that into legislation. The proposals deal with this in various ways. As we heard from Congressman Shays, authorization would only be required where people were consenting to use for research. I don't really think that that is as comprehensive an approach as we need. My view is that we should build consent and notice into all disclosures except for certain limited exceptions, such as public health, emergency, law enforcement where there's a warrant, and research where there is an IRB approval process in place.

On the research issue, I think it's important to note that we already have a set of Federal regulations that govern federally fund-

ed researches that require an institutional review board to assess the efficacy of the research project as it moves forward. It requires informed consent, but there's a waiver provision in there that allows the IRB to assess where getting informed consent would be very difficult, and where it would impede the research project as it goes forward. I think we need to take a look at those regulations, and look at applying them to the private sector as well, which doesn't currently have similar protections in place.

Security is a big issue which has been mentioned at all of the pending proposals. We need to require that there be safeguards in place to protect personal information.

On law enforcement, I think other than the administration, there is broad agreement that law enforcement should be required to present some legal process, either a court order or a warrant before getting access to medical records. The Video Privacy Protection Act requires that, as does the Right to Financial Privacy Act. In the bill put forward by Senators Jeffords and Dodd, it does require the same level of protection and the same court process that the Video Privacy Protection Act requires, and a number of the other proposals also incorporate that.

On remedies, again, there is very broad agreement on remedies that we need to have strong, enforceable remedies and penalties in place for misuse of information. Some of the proposals don't include punitive damages, but that's really the main area where there's been some disagreement.

Preemption, I think, is in some way the largest issue and the toughest one that we've had to wrestle with. I would suggest that in some ways it makes sense to reserve that issue until the end of the debate given if the legislation that is agreed upon by Congress is strong enough and sets the bar high enough. In some ways the preemption issue becomes moot then, because it will supersede in strength any laws that do exist at the State level.

You had asked if last year, Mr. Chairman, about California's law. In looking at that law, it is very broad and far-ranging in terms of consumer protection and privacy, and is very specific. So I would be concerned about wiping out laws where we don't already know what those laws require and what their scope is. As I've said, our project is putting together a compendium, so we can make a more informed decision as we get to the end of this debate.

To borrow from a phrase that Congressman Shays used in his opening statement, he says "that most of the answers lie somewhere in between," and while I don't want to suggest what that "in between" is yet, I think we all need to be committed to a process where we hear each other, we look at the various views, we create a factual record, and we're able to move forward and give the American public what it needs, what it's been demanding which is a strong, enforceable health privacy law.

Thank you very much.

[The prepared statement of Ms. Goldman follows:]

I. INTRODUCTION AND OVERVIEW

Mr. Chairman and Members of the House Subcommittee on Government Management, Information, and Technology of the Committee on Government Reform and Oversight: I very much appreciate the invitation to testify before you today on patient confidentiality.

In December 1997, I launched the Health Privacy Project at the Institute for Health Care Research and Policy at Georgetown University Medical Center. Prior to creating the Project, I have focused on privacy and technology issues — particularly health privacy— for over a decade, as co-founder and Deputy Director of the Center for Democracy and Technology, and as Director of the Privacy and Technology Project of the American Civil Liberties Union.

At present, there is no comprehensive federal law to protect the privacy of peoples' health records. I believe health privacy is one of the most important health issues facing our nation: it is critical to improving health care, and fostering valuable public health initiatives. Fortunately, Congress recognized the urgent need for enforceable health privacy rules, and set itself a time limit in the Health Insurance Portability and Accountability Act of 1996 to pass health privacy legislation by August 1999.

While there is often broad agreement on the principles of health privacy, we have not yet been able to reach consensus on the implementation of many of these principles. The Health Privacy Project was established to raise public awareness of the importance of health privacy to improving health care in this country, both on an individual and a community level. Our work is focused in three areas: the Project is staffing a Health Privacy Working Group comprised of diverse stakeholders in the health care and consumer communities in an attempt to reach common ground on "best principles;" the Project is preparing a compendium of state health confidentiality laws; and the Project is identifying models within the health care community for health privacy "best practices."

The primary goal of the Health Privacy Working Group is to define a set of "best principles" for health privacy. The final principles will be supported by a fact-intensive report that will serve as a record of how information is gathered and used for various health care initiatives such as research, public health, outcomes analysis, and providing and paying for health care. Members of the Working Group include: disability and mental health advocates; health plans; providers; employers; standards and accreditation organizations; researchers; a pharmaceutical company; and experts in public heath, medical ethics, information systems, and health policy.

My statement today will outline the need for a comprehensive health privacy law. I urge that we embrace a new framework that views protecting privacy in the health care arena as an ultimate

good, which will advance two key goals: 1) foster patient trust and confidence in the doctor/patient relationship, and 2) enhance the quality of patient data needed for improving patient care, research, and public health initiatives. Applying this framework, I provide preliminary comments on House and Senate bills, including The Consumer Protection and Medical Record Confidentiality Act of 1998, discussion draft (5/14/98) authored by Representative Chris Shays (R-CT). First, I include an overview of health privacy and the public's need and demand for a strong, workable, federal health privacy law.

II. PUBLIC NEED AND DEMAND FOR HEALTH PRIVACY

A lot of attention has been paid in recent years to how to improve health care in this country, but a critical element that is often overlooked and misunderstood is the role privacy and confidentiality plays in the health care setting. Nearly every facet of health care — including health care delivery, payment, prescribing medication, outcomes analysis, research, and marketing — is undergoing dramatic changes as our society moves towards managed care and the development of integrated health data networks. As a recent editorial in The New York Times observed, "Preserving privacy in the ever-expanding world of electronic medical records is a daunting task that health care organizations and public policy makers have been slow to address. But as managed care puts more information into more hands, consumer anxiety over confidentiality makes the issue unavoidable."

Americans are becoming increasingly aware that the broad waivers they sign as a condition of payment and treatment leave them vulnerable to a wide array of uses and reuses of their personal health information. Once information is collected for one purpose, the temptation to use it for other purposes is often irresistible.

Recent press reports about the widespread disclosure of personal health information has fueled the public's concern about the lack of protections. Most recently, the chain drug stores CVS and Giant Food admitted to disclosing patient prescription records to a direct mail and pharmaceutical company. Their stated intent was to track customers who don't refill prescriptions, and send them letters encouraging them to refill, and consider alterative treatments. However, in response to the outrage and worry expressed by their customers, both companies subsequently advertised their plans to abandon their marketing and direct mail campaigns ("Prescription Fear, Privacy Sales," Washington Post, p. A1, 2/15/98).

The key issue here is not the primary, expected use of one's medical records — to provide care and pay health care claims — but the secondary, unanticipated uses of personal health information. Routine disclosures of personal health information may be more common than initially understood:

- Medical Marketing Service advertises a database available to pharmaceutical marketers which includes the names of 4.3 million people with allergies; 923,000 with bladder control problems; and 380,000 who suffer from clinical depression. (See www.mmslists.com)

- A recent article discussing new demands for health data explained that "Data can come from a variety of sources, such as pharmacy and/or medical claims, patient or provider reports, and patients' charts... At PCS, the outcomes research group has online access to 700 million pharmacy claims, which represent the past 25 months of prescriptions filled. The information on a prescription becomes available online within 48 hours after the pharmacist dispenses it." ("Translating Data into Useful Information: The Evolving Role of the PBM, Drug Benefit Trends, 1998)

- An Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol ("Many Can Hear What You Tell Your Doctors: Records of Patients Are Not Kept Private," Orlando Sentinel, 11/30/97, A1)

The public has consistently expressed a high degree of concern over the vulnerability of their privacy, in particular the lack of protection for their personal health information. Decades of survey research conducted by Louis Harris & Associates document a growing public concern with privacy. The 1995 Harris poll found that 82% of people were concerned about their privacy, up from 64% in 1978. Nearly sixty percent (60%) of the public have at some point "refused to give information to a business or company" out of concern for privacy, up from forty percent (40%) in 1990.

A Health Information Privacy Survey released by Harris in 1993 found that twenty-seven percent (27%) of the public believe that their personal medical information was disclosed improperly. Of these people, thirty-one percent (31%) believe they were harmed or embarrassed by the disclosure. When health care leaders were asked if they knew of violations of patient confidentiality from within organizations, 24% reported that they did, and could describe the violations in detail.

In order to protect their privacy, eleven percent (11%) of the public have on occasion chosen not to file an insurance claim. Seven percent (7%) chose not to seek care because they didn't want to harm their "job prospects or other life opportunities."

Harris' 1996 survey highlighted the public's desire to keep medical information private. Of all the person information collected by businesses, medical records, and pharmaceutical data were considered the most sensitive. For example, only eighteen percent (18%) consider the use of patient records for medical research without prior permission to be very acceptable. Only twenty-five percent (25%) of the public found it acceptable to use prescription data to detect fraud. In the 1993 survey, sixty percent (60%) found it not acceptable for pharmacists to provide patient information to marketers without patient approval.

Harris' 1993 survey found that the majority of the public (56%) favored the enactment of strong comprehensive federal legislation to protect the privacy of health care information. In fact, of that majority, eighty-five percent (85%) responded that protecting the confidentiality of medical records was absolutely essential or very important to them. An overwhelming percentage wanted penalties imposed for unauthorized disclosure of medical records (96%), guaranteed access to their own records (96%), and rules regulating third-party access to personal health information.

The reason for this level of concern is clear: medical records contain intimate, highly sensitive personal information such as family history; testing; diagnosis and treatment of illness and diseases; drug and alcohol use; sexual history; and medications prescribed. Despite the sensitive nature of the records today, it is far easier for others to get access to medical records than it is to credit reports, or even video rental records. Consider the following:

- After news of actress Nicole Kidman's recent surgery was leaked to the press, photos of her leaving the UCLA Medical Center appeared in papers with commentary about her health status. (Parade Magazine, May 10, 1998)

- In a recent survey, 206 respondents reported discrimination as a result of access to genetic information, culminating in loss of employment and insurance coverage, or ineligibility for benefits. (Science and Engineering Ethics, 1996)

- In Tampa, a public health worker walked away with a computer disk containing the names of 4,000 people who tested positive for HIV. The disks were sent to two newspapers. (USA Today, October 10, 1996)

- A recent survey found that 35% of Fortune 500 Companies look at people's medical records before making hiring and promotion decisions. (Unpublished study, University of Illinois at Urbana-Champaign, 1996)

- The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. Following a series of press reports describing the system, the HMO revamped its computer security practices.

- A banker who also served on his county's health board cross referenced customer accounts with patient information. He called due the mortgages of anyone suffering from cancer. (The National Law Journal, May 30, 1994)

- New York Congresswoman Nydia Velasquez' confidential medical records — including details of a bout with depression and a suicide attempt — were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary. After overcoming the fallout from this disclosure and winning the election, Rep. Velasquez testified eloquently about her experiences before the Senate Judiciary Committee as it was considering a health privacy proposal.

- In Maryland, eight Medicaid clerks were prosecuted for selling computerized record printouts of recipients' and dependents' financial resources to sales representatives of managed care companies.

- The 13-year-old daughter of a hospital employee took a list of patient's names and phone numbers from the hospital when visiting her mother at work. As a joke, she contacted patients and told them that they were diagnosed with HIV. (The Washington Post, March 1, 1995)

- The director of a work site health clinic operated by a large manufacturing company testified that he was frequently pressured to provide personal information about his patients to his supervisors.

- The late tennis star Arthur Ashe's positive HIV status was disclosed by a health care worker and published by a newspaper without his permission.

Focusing specifically on mental health care, a New York Times Magazine article, "Keeping Secrets," observed: "[A]t present it is unrealistic for people to assume that the raw and tender subjects they talk over with their therapists will go no further than the four walls of the consulting room. And many patients have become legitimately concerned about the possibility that the depression, suicide attempt, marital problem or alcoholism being discussed could return to haunt them in cyberspace. They are uncomfortably aware of the shadowy figures sitting in on their therapy sessions: the insurance administrator, the electronic file clerk, the case reviewer, other physicians with an H.M.O.—even their own co-workers and supervisors ." (June 16, 1996, p. 38)

III. PROTECTING PRIVACY TO IMPROVE HEALTH CARE

Initiatives to improve public health and reshape health care — such as community health information networks, managed care, telemedicine, outcomes analysis, disease management, the creation of population databases — could not exist, let alone flourish, without access to complete and reliable information. Some fear that addressing privacy at the patient level will threaten these new health care initiatives. They fear that protecting privacy will clog the free flow of health information, and make less information available for outcomes analysis, research, public health activities, and other health-related purposes.

Ultimately, the converse is true: **without trust that the personal, sensitive information they share with their doctors will be handled with some degree of confidentiality, patients will not fully participate in their own health care**. Along the continuum, if doctors and other health care providers are receiving incomplete, inaccurate information from patients, the data they disclose for payment, research, public health reporting, outcomes analysis, and other purposes, will carry the same vulnerabilities. Therefore, protecting privacy must be an integral part of both ensuring good health care to individuals and improving the health of the larger community.

In many ways, the relationship between people and their doctors bears the greatest burden in the health privacy debate; this relationship is the "hot spot," the originating point on the health information continuum. It is in the first and subsequent encounters with a particular provider that a person decides how much to divulge, and whether that provider can be trusted. Concerns about privacy are one of the reasons why a patient may not fully and accurately disclose to their provider.

If people do not trust that their most sensitive information will be treated confidentially by their doctors, and may be disclosed without their knowledge and permission to their employers, pharmaceutical companies, or marketers, these people are likely to engage in "privacy-protective" behavior. In order to protect their privacy, patients may pay out-of-pocket for medical care, "doctor-hop" to avoid having all their health information entrusted to one provider, withhold information, lie, or even avoid care altogether. People fear compromising their privacy, or suffering negative consequences such as embarrassment, stigma, and discrimination.

The consequences of such privacy-protective behavior for patients, as well as the health care initiatives intended to serve them, are significant:

- The patient may receive poor quality of care, risking untreated and undetected health conditions.

- The doctor's abilities to diagnose and treat accurately are jeopardized by a lack of complete and reliable information from the patient.

- The integrity of the data flowing out of the doctor's office is undermined. The information the patient provides, as well as the resulting treatment and diagnosis, may be incomplete and inaccurate, and not fully representative of the patient's care or health status.

- A doctor may skew diagnosis or treatment codes on claim forms, or the doctor may keep separate records to be maintained and kept within the doctor's four walls, and send on incomplete information for claims processing in order to encourage a patient to more fully communicate.

- The credibility of any research or analysis performed in reliance on the patient's data is called into question. If the patient's health data is unreliable from her medical record and claims data, the downstream user (researcher, public health official) lacks any information as to where the information might lack integrity or why. In other words, there may be no clue in the record that something is missing or false.

In the health care setting, when patients withhold information or shun care to protect their privacy, they must do so with a broad, undiscriminating brush — they have to calculate for every negative possibility. But, if people are assured that their health information will be safeguarded, and if they are empowered to make informed, voluntary choices about the secondary use of their health information, people are likely to seek care, more fully open up to their health care providers, and make educated decisions about the disclosure and use of their personal health information.

I urge that we abandon the current dialogue that places privacy and public health initiatives in conflict. A new framework is needed that intertwines the values of protecting patient privacy and fostering health care initiatives. At this juncture, let us treat patient privacy as a "first principle" of ensuring quality of care for individuals and their communities. Ideally, within such a health privacy framework, identifiable information patients choose to disclose outside the four walls of their doctor's offices would be more accurate and complete, and thus create more reliable data for use by doctors, researchers, and others working to enhance the quality of health care. By expanding our focus to incorporate privacy as an ultimate good to be achieved in the health care arena, we may better advance our health care initiatives.

IV. CONSENSUS FOR A NATIONAL HEALTH PRIVACY POLICY

Protecting privacy and promoting public health initiatives are values that must — and can — go hand-in-hand. First recognized in the Hippocratic oath more than 500 years ago, confidentiality has long been a central tenet of the doctor-patient relationship. Most recently, the Presidential Advisory Commission on Consumer Protection and Quality in the Health Care Industry issued its recommendations for a "Patients' Bill of Rights," which states: "individual patients' medical records should be treated confidentially, and disclosed only in order to treat them and pay bills."

A consensus exists among the public, policymakers, and a broad spectrum of the health care field that a comprehensive health privacy policy is needed in this country. As a recent editorial in The Washington Post concluded: "Of all the threats posed to personal privacy by new information technologies, the threat to the privacy of medical records is by the far the most urgent." ("Medical Files, or Fishbowls?" 9/23/97, p. A16)

Reports of the last twenty years are unanimous in concluding that a comprehensive national health privacy law is critical to ensuring both the integrity of the doctor/patient relationship and the continued development of this nation's health care system (See For The Record: Protecting Electronic Health Information, National Research Council, 1997; Health Data in the Information Age: Use, Disclosure and Privacy, National Academy of Science, Institute of Medicine, 1994; Protecting Privacy in Computerized Medical Information, Office of Technology Assessment, 1993). In the past few years, every witness that has testified before the U.S. Congress has stated that a comprehensive federal privacy law is critical to preserving peoples' trust in their doctors and in the health care system.

S. 1360, The Medical Records Confidentiality Act of 1996 introduced last Congress by Senators Bennett and Leahy, quickly garnered broad bi-partisan support, including co-sponsorship by Senators Dole, Daschle, Kassebaum, Kennedy, Jeffords, and Frist. Despite this powerful hand holding, agreement on the scope and implementation of a national health privacy policy continues to present a challenge.

We now have a new and promising opportunity for meeting this challenge. The recently enacted Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes a provision mandating that either Congress or the Secretary of HHS establish an enforceable privacy regime to protect personally identifiable health information. (P.L. 104-191, also known as Kassebaum-Kennedy) In HIPAA, Congress set itself a time limit of August, 1999 for enacting a health privacy

law. If Congress fails to act by that time, the Secretary of HHS is required to promulgate health privacy regulations by January, 2000.

To provide some guidance for legislation, HIPAA required the Secretary to submit to Congress her blueprint for health privacy legislation. In September 1997, Secretary Shalala issued a set of recommendations to Congress to "enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who serve them." The Secretary's recommendations parallel to a large extent the recommendations of other national bodies, as well as incorporating approaches taken by many of the proposed medical confidentiality bills introduced in Congress over the past. The major recommendations are to:

- Impose new restrictions on those who pay and provide for care, as well as those who receive information from them. It should prohibit disclosure of patient-identifiable information except as authorized by the patient or as explicitly permitted by the legislation. Disclosures of identifiable information should be limited to the amount necessary to accomplish the purpose of the disclosure, and should be used within an organization only for the purposes for which the information was collected.

- Provide consumers with significant new rights to be informed about how their health information will be used and who has seen that information. Providers and payers should be required to advise patients in writing of their information practices. Patients should be able to see and get copies of their records, and propose corrections. A history of disclosures should be maintained by providers and payers, and be made accessible to patients.

- Provide for punishment for those who misuse personal health information and redress for people who are harmed by its misuse. There should be criminal penalties for obtaining health information under false pretenses, and for knowingly disclosing or using medical information in violation of the Federal privacy law. Individuals whose rights under the law have been violated should be permitted to bring an action for damages and equitable relief.

Secretary Shalala concludes that "without safeguards to assure that obtaining health care will not endanger our privacy, public distrust could turn the clock back on progress in our entire health care system." (Shalala report, pp 1,2.)

However, the Secretary's report drew fire from the Hill, the media, health care providers, and health privacy experts for her recommendation that law enforcement officials continue to have virtually unfettered access to personal health records. As The New York Times editorial decried: "The exemption for law enforcement agencies is a huge loophole.. The need to combat fraud in the nation's trillion-dollar health-care industry is indisputable. But it hardly justifies granting less privacy protection to the intimate information contained in medical records than existing Federal

statutes now extend to the records of banks, cable television, video rental stores, or E-mail users, as the Administration's plan bizarrely contemplates." (See "Trifling with Medical Privacy," 9/97)

No other federal privacy statute provides such an exemption for law enforcement. In fact, most of the U.S. privacy laws were enacted specifically to bring law enforcement under a Fourth Amendment warrant mandate.

It is also worth noting that HIPAA includes a provision known as "Administrative Simplification." Coupled with the law's privacy mandate is a requirement that uniform health data standards for the electronic transmission of personal health data be developed. The first set of draft regulations were just made public by HHS on May 7, 1998. The consequence of these dual and staggered requirements is that a time line has been established by which data standards must be created *prior* to the development of privacy and security rules governing personal health information. Both the short time frame and the awkward sequence of events laid out in the "Administrative Simplification" section pose unique challenges for health care entities, policymakers, and patients.

V. KEY ISSUES FOR A FEDERAL HEALTH PRIVACY POLICY

There are a number of proposals pending before the House and Senate with regard to medical privacy. In the House, under consideration are: the "Consumer Protection and Medical Record Confidentiality Act of 1998," (discussion draft 5/14/98) authored by Representative Chris Shays(R-CT); "Medical Privacy in the Age of New Technologies Act of 1997" (H.R. 1815), introduced by Representative Jim McDermott (D-WA); and the "Fair Health Information Practices Act of 1997" (H.R. 52), introduced by Representative Gary Condit (D-CA).

In the Senate, under consideration are: "The Health Care Personal Information Nondisclosure Act of 1998," (S. 1921) co-authored by Senator James Jeffords (R-VT) and Senator Chris Dodd (D-CT); "The Medical Information Protection Act of 1998," (discussion draft 2/19/98) authored by Senator Robert Bennett (R-UT); and "The Medical Information Privacy and Security Act, " (S. 1368) introduced by Senator Patrick Leahy (D-VT) and Senator Edward Kennedy (D-MA).

In addition, Congress has held several hearings on medical privacy in the past few months including a hearing March 24, 1998 by a subcommittee of the House Committee on Ways and Means, and a Senate Committee on Labor and Human Resources hearing on February 26, 1998.

The congressionally mandated time limit to pass health privacy legislation by August 1999 shifts the political landscape, and injects greater immediacy into the effort to find a strong, workable privacy solution. Many of the health privacy proposals currently pending before Congress address,

in various ways, a set of key principles and approaches, which are also echoed in recent federal reports and studies mentioned earlier in this statement.

The following is a broad outline of the elements that should be incorporated in a comprehensive health privacy policy.

A. Access

People should have the right to see, copy, and supplement their own medical records. Only 28 states currently provide such a right.

Pending Proposals

All of the bills introduced in the House and Senate provide patients with a right to see and copy their medical records. All the bills allow entities to charge fees for copying, and all, except S. 1368, outline limited exceptions to a patient's right of access.

B. Notice

People should be given written, easy-to-understand notice of how their health information will be used and by whom. Only with such notice can people make informed, meaningful choices about uses and disclosures of their health information.

Pending proposals

All of the bills introduced in the House and Senate require that patients be given notice about the uses of their personal health information.

C. Consent

As a general rule, patient consent should be obtained prior to disclosure of personal health information by doctors, health plans, employers, and other health care entities, especially if the disclosure is not related to treatment or payment. There seems to be a broad recognition that exceptions to the rule of consent are needed for certain public health disclosures and in emergency circumstances.

Pending proposals

All of the bills introduced in the House and Senate require, as a general rule, patient consent prior to disclosure. The bills differ with regard to exceptions to this rule (see, in particular, the analysis below about access for researchers and law enforcement).

Most bills provide for a two-tiered authorization process. For instance, within the first level of authorization, a health care entity can require consent for certain uses of personal health information as a condition of receiving care or providing payment. Generally, the second tier authorization is for disclosures not related to treatment and payment, and allows patients to refuse to authorize disclosures, and continue to receive care and payment, without suffering any adverse consequences for withholding such authorization.

- The Shays draft does not require an authorization for disclosures related to treatment, payment, and certain health care operations. The draft does require an authorization for most other disclosures.
- S. 1368 and H.R. 1815 define this first tier as covering disclosures necessary for "treatment and payment" only. Only S. 1368 allows patients to self-pay in order to avoid any disclosure for payment purposes.
- S. 1921 includes "health care operations" in the first level of authorization, along with payment and treatment.
- H.R. 52 defines the first tier of authorization to include disclosures for health care, payment, or for use by a health care oversight agency.

D. Research

A federal privacy law should strengthen and expand the reach of existing privacy safeguards for identifiable health information used by researchers. Overall, a national health privacy policy should create incentives for researchers to use non-personally identifiable health data.

Specifically, there should be equity, uniformity, accountability and oversight in scope and application of the federal regulations governing Human Subjects research and the use of personally identifiable health information by researchers. Regulations should be applied to both federally and non-federally funded researchers, and the existing standard for granting

waivers of informed consent for use of identifiable data should be codified, strengthened and strictly applied.

Pending proposals

- The Shays draft requires, as a general rule, that researchers either obtain approval from an Institutional Review Board (IRB), or enter into a confidentiality contract with the disclosing entity, prior to receiving identifiable health information
- S. 1368, H.R. 52, and H.R. 1815 all require approval by an (IRB) prior to using personally identifiable data in a research project. Under the federal regulations referenced in these bills, the IRB can waive the informed consent requirement if the potential benefit of the research is determined to outweigh the privacy interest of the individual.

E. Security

It is important to require the development of security safeguards for the use and disclosure of personal health information. While it is critical to acknowledge that networked health information systems can pose a risk of greater magnitude and harm, technology can be used to better safeguard personal health information in electronic form than it would be protected if on a piece of paper in a file drawer (see For the Record: Protecting Electronic Health Information, National Research Council, 1997). No system — either paper or electronic — can provide 100% fool-proof security, but the technology does provide us with some powerful opportunities to better protect personal information. Also, technology can be used to more efficiently anonymize and de-identify personal health data for public health initiatives.

Pending proposals

All of the bills in the House and Senate require health care entities to establish safeguards to protect personally identifiable health information. Only S. 1368 allows for patients to opt out of having their personal health information entered in electronic form. Such an "opt-out" may create a false expectation that sensitive information is better protected in paper form. Again, this is not necessarily true if strong security policies and tools are built in to information systems.

F. Law Enforcement

A federal health privacy law should include a court order requirement, with a standard as stringent if not more so than that set out in the Video Privacy Protection Act (better known as "The Bork Bill"). Constitutional principle requires that individuals should be shielded from unjustified government intrusion. Currently, no federal privacy statute provides a broad exemption for law enforcement. In fact, most of the U.S. privacy laws were enacted specifically to bring law enforcement under a Fourth Amendment warrant mandate.

Pending proposals

All of the pending proposals require some form of legal process, with a standard, prior to disclosure to law enforcement officials. However, the proposals vary widely on the standards to be applied i.e. S. 1368 and H.R. 1815 allows for disclosure to law enforcement pursuant to a court order or subpoena that meets a "clear and convincing" standard; H.R. 52 and S. 1921 requires law enforcement to meet a probable cause standard; and the Shays draft requires that law enforcement first find that the need for the information substantially outweighs the privacy interest of the individual.

G. Remedies

In order to be truly effective, a federal health privacy law must have strong remedies in place. For instance, strict civil penalties and criminal sanctions should be imposed for violations of the law, and individuals should have a private right of action against those who mishandle their personal medical information.

Pending proposals

All of the bills, with certain differences introduced in the House and Senate provide strict civil penalties, criminal sanctions, and a private right of action for individuals. A number of the proposals do not allow for punitive damages to be awarded.

H. Preemption

No precedent exists in our federal privacy and civil rights laws for preempting state law. In the case of health privacy, we do not yet have a comprehensive survey of state law that would even indicate *what* state laws we would be preempting. Further, health care entities

are currently doing business and transferring information interstate, complying with various state health privacy laws.

Serious consideration should be given to any proposal to preempt state law in this area, thereby locking the states out of tailoring their laws to reflect particular circumstances. For instance, stronger state mental health and communicable disease confidentiality laws should not be preempted, given the long history of stigma and discrimination against people with these conditions. Moreover, given what we know of the resistance to testing and accessing treatment, these state privacy laws help to promote broad public health interests.

Pending proposals

- S. 1368 and H.R. 1815 do not preempt any state law that provides a greater level of protection for personally identifiable health information.
- S. 1921, H.R. 52 and the Shays draft preempt state law with limited exceptions, most notably state laws with regard to mental health, public health, communicable disease, and the reporting of vital statistics, abuse or neglect.

VI. CONCLUSION

I am optimistic that the political will exists this Congress to pass legislation that truly protects peoples' privacy in the health care setting, without unduly compromising valuable health care initiatives. The time has come for a cohesive, forward-thinking health privacy paradigm that acknowledges privacy's critical role in health care, and integrates it at various states throughout the health care system. People must be empowered to be more active, informed consumers of health care and knowing, willing participants in the broader health care activities that impact their lives and well-being of their communities. If we are to achieve the oft-touted goals in health care, people must have trust and confidence that the health care system will safeguard their personal health information. Loss of personal privacy – and ultimately the erosion of reliable health information – must not be the price of progress.

Mr. HORN. Well, we thank you very much for your very thorough tatement and your filed document.

I might say to all of you that your remarks are automatically iled in the record once we introduce you. You don't have to read verything, just summarize it so we can have a dialog between the even of you and whoever is here on the dias, given all the other ommittee commitments they have.

You've certainly cited some horrible examples, such as the one rom the Washington Post, of the little young lady, 13 years of age, hat started phoning people and telling them they were diagnosed /ith HIV. That's certainly a commentary on someone taking med- :al records home, not intending for that to happen, and the dan- ers it has because of somebody's perverted, weird kind of humor.

So, now we have Mr. Nielsen. We appreciate you coming here, nd look forward to your testimony. Now, you are the senior coun- el director of government affairs for Intermountain Health Care, nc., and we're glad to have you. Will you summarize your testi- ıony?

Mr. NIELSEN. Thank you, Mr. Chairman, Congressman Davis— guess he's left.

I'm testifying today not on behalf of my employer, but on behalf f the American Hospital Association. Every day thousands of pa- ients walk through the doors of America's hospitals, each provide heir caregivers with information of the most sensitive and inti- ıate nature. Our members consider themselves guardians and ustodians of this information, and that is the reason that the ımerican Hospital Association supports strong Federal legislation ɔ establish uniform national standards for the use of patients' per- onal medical information. We refer to that as protected health in- ɔrmation.

I've been asked to discuss the Consumer Protection and Medical :ecords Confidentiality Act as authored by Representative Shays. Ve've also been asked to discuss legislation introduced by Senator effords as well. The Jeffords bill is based upon an earlier draft of proposal by Senator Robert Bennett which has not yet been intro- uced at this time. We've also been requested to comment on how hese proposals address three areas: authorizations for the use of rotected health information; preemption of State law; and, defini- ions of what areas of health care delivery need access to that in- ɔrmation.

The draft being developed by Senator Bennett, and the bill intro- uced by Senator Jeffords reflect a permissive approach. That is, hey define when a health care provider or a system should be able ɔ use protected health information with few exceptions considered isclosure for other purposes, a violation of the law. Senators Ben- ett and Jeffords would require a patient to sign an authorization llowing health information to be used for specific purposes such s treatment, payment, and health care operations, as those terms re defined.

I think, as the chairman has recognized, Representative Shays ıkes a different approach. His proposal identifies prohibited uses f protected health information, then carves out exceptions in an ffort to allow care to be provided and paid for without the need ɔr specific authorization. However, Representative Shays' proposal

does require authorizations if the information is to be disclosed for purposes other than those carved out as exceptions.

We believe that Representative Shays' current approach may lead to uncertainty in determining when providers need to secure an authorization. This approach, coupled with the strong sanctions contained in the legislation could encourage providers to obtain multiple authorizations throughout the treatment process, even when not required, potentially affecting the timeliness of delivery of health care.

AHA believes strong preemption of State law is critical. Some exceptions are appropriate, such as in the area of public health; however, they should be specific and very clearly stated as they are in the latest Bennett draft. Leaving in place State laws that fall under the rubric of public health or mental health will require patients, providers, and health plans to comply with a variety of confusing and potentially conflicting requirements.

AHA supports the specificity with which the Shays bill outlines public health laws that are not preempted. However, carving out other categories of health care information does not promote the goal of nationally consistent rules governing the disclosure of protected health information as supported by the American Hospital Association.

We're also concerned that the definitions in the Shays bill do not appear to recognize a growing necessity of today's integrated health care environment. That is, the need to coordinate health care across a variety of different settings. It also omits specific reference to many other functions that are central to quality care, such as outcomes, evaluations, disease, and case management. In the Jeffords bill, these functions are summed up in the combined definition of treatment, payment, and health care operations. The Bennett proposal is even more specific and descriptive of these critical functions.

We believe these concepts and functions must be captured in the definition section of proposed legislation, and also should be included as exceptions to the prohibitions on use and disclosure.

The issue of law enforcement use of protected patient information is not a focus of this hearing, but we feel that we ought to address it briefly. We are still evaluating all of the legislative proposals as to how they treat this important issue. However, AHA strongly believes that protected health information should be available to law enforcement agencies only after a request has been made through a process that involves a neutral magistrate or through other processes that involve court oversight.

In conclusion, the AHA applauds Representative Shays, and all of the other Senators and Representatives who have turned their attention to this critical issue and that are working on much-needed Federal legislation. We share the goal of protecting the confidentiality of the patients we serve, while also ensuring that the free flow of information, which is so central to the optimal delivery of health care, is not impeded.

We look forward to working with the subcommittee and others interested in this issue, and would be pleased to answer any questions. Thank you.

[The prepared statement of Mr. Nielsen follows:]

Testimony
of the
American Hospital Association
before the
Subcommittee on Government Management, Information, and Technology
of the
Committee on Government Reform and Oversight
of the
United States House of Representatives
on
Medical Privacy Legislation

May 19, 1998

Mr. Chairman, I am John T. Nielsen, senior counsel and director of governmental affairs for Intermountain Health Care Inc. (IHC). IHC is an integrated health care system based in Salt Lake City, Utah. IHC consists of 23 hospitals, 33 clinics, 16 home health agencies, and 300 employed physicians. We also have a large Health Plans Division with an enrollment of 350,000 members. I am testifying today on behalf of the American Hospital Association (AHA), which represents nearly 5,000 hospitals, health care systems, networks, and other providers of care. We appreciate this opportunity to present our views on an issue of critical importance to our members and the patients they care for: the confidentiality of protected health information.

Washington, DC Center for Government and Public Affairs
Chicago, Illinois Center for Health Care Leadership

Liberty Place, Suite 700
325 Seventh Street, N.W.
Washington, DC 20004-2802
(202) 638-1100

Protecting patients' trust

Every day, thousands of Americans walk through the doors of America's hospitals. Each and every one of them provides caregivers information of the most intimate nature. They provide this information under the assumption that it will remain confidential. It is critical that this trust be maintained. Otherwise, patients may be less forthcoming with information about their conditions and needs -- information that is essential for physicians and other caregivers to know in order to keep people well, ease pain, and treat and cure illness.

If caregivers are not able to obtain and share patients' medical histories, test results, physician observations, and other important information, patients will not receive the most appropriate, high-quality care possible.

Our members consider themselves guardians of this information. That is why AHA has long supported the passage of strong federal legislation to establish uniform national standards for all who use patients' personal medical information -- what we will refer to as protected health information.

It's an issue that affects all of us personally. We live in a time of rapidly advancing technological improvement, when the world seems to get smaller as computers get more powerful and databases get bigger. This technological change can be positive -- it has led to significant improvements for both health care providers and their patients -- but it worries people who are justifiably concerned about how information about them will be used.

In health care, we must take the steps necessary to protect that information from those who would misuse it. We need strong, uniform federal legislation to do it.

Our goals for legislation

First and foremost, because we as hospitals and health systems put our patients first, we must restore and maintain people's trust in the privacy and confidentiality of their personal health information. Federal legislation can do this by establishing a uniform national standard for the protection of this information -- including genetic information -- a standard that balances patient privacy with the need for information to flow freely among health care providers. The AHA believes that federal confidentiality legislation must meet the following goals:

- Allow patients and enrollees access to their medical information, including the opportunity, if practical, to inspect, copy, and, where appropriate, add to the medical record. Patients have a right to know what information is in their records. This level of accountability encourages accuracy and has the added benefit of encouraging patient involvement in their care.

- Preempt state laws that relate to health care confidentiality and privacy rights, with the exception of some public health laws. Health care today is delivered through providers that are linked together across delivery settings, and in organizations that cross state boundaries. AHA believes that the best way to set important standards for confidentiality of protected health information is to do so uniformly -- through a strong federal law. This

law must be both a floor and a ceiling, preempting all state laws with which it may conflict, weaker or stronger. Only through such a uniform law can patients' health information be equally protected regardless of the state in which they live or travel.

- Be broad in its application, covering all who generate, store, transmit or use protected health information, including but not limited to providers, payers, vendors, and employers. Patient confidentiality cannot be ensured unless standards are applied to all who may have access to their health information. Legislation should cover all types of protected health information, including sensitive issues such as substance abuse, mental health, and genetic information.

- Strike an appropriate balance between patient confidentiality and the need to share clinical information among the many physicians, hospitals and other caregivers involved in patient care. Care is increasingly provided by groups and systems of providers as opposed to individual providers. These new systems create opportunities for real improvements, but they rely heavily on a free flow of information among providers. Patient confidentiality is of the utmost importance. But in order to ensure that care can be coordinated and the patient's experience is as seamless as possible, information must be accessible to all providers who treat the patient.

- Recognize that a hierarchy of need exists among users of protected health information. Access to individually identifiable information is essential for patient care. Such access

may also be necessary for provider and health care system efforts to measure and improve the quality of care. All internal and external uses of protected health information must be evaluated as to whether they are justified.

To limit its potential misuse, all within the health system should restrict the availability of protected health information. Technology is available to do this, through encryption, audit trails, and password protection, for example. Another method for restricting the availability of protected health information is to aggregate information whenever possible. Patients should be assured that unique, identifiable information about them is available for their treatment, but that its availability for other uses is tightly controlled.

- Include sufficient civil and criminal penalties to deter inappropriate disclosure of protected health information. The level of such sanctions should vary according to the severity of the violation. At the same time, any penalty imposed must take into account good-faith efforts by providers who establish data safeguards, educate employees about complying with the safeguards, and attempt to maintain secure record-keeping systems.

The Consumer Protection and Medical Record Confidentiality Act of 1998

Several bills on protected health information have either been introduced or are being prepared for introduction. We have been asked to focus on the most recent discussion draft of the Consumer Protection and Medical Record Confidentiality Act of 1998, authored by Rep. Chris Shays (R-CT), and include comparisons to other confidentiality legislation, including the Health Care

Personal Information Nondisclosure Act of 1998 (S. 1921), introduced by Sen. Jim Jeffords (R-VT). The Jeffords bill is based on an earlier draft of a proposal by Sen. Robert Bennett (R-UT), which has not yet been introduced.

Authorizations

Rep. Shays' proposal and the respective proposals of Sens. Bennett and Jeffords represent two distinct approaches to achieving the same goal: protecting patient confidentiality. The draft being developed by Sen. Bennett and the bill introduced by Sen. Jeffords reflect a "permissive" approach. That is, they define the purposes for which a health provider or system should be able to use protected health information and, with few exceptions, consider disclosure for other purposes to be a violation of the law.

To ensure that a health plan enrollee understands how his or her health information will be used, Sens. Bennett and Jeffords would both require the individual to sign an authorization allowing the information to be used for specific purposes -- such as treatment, payment and health care operations. They then outline parameters for external disclosure of the information, such as research and law enforcement. Some external disclosures are allowed without authorization -- such as emergencies, identification of bodies, and the reporting of abuse.

This approach ensures confidentiality within a health care system by requiring the establishment of safeguards to minimize the number of people who might see or use protected health information.

Rep. Shays takes a different approach. His proposal attempts to identify prohibited uses of protected health information, and then carves out exceptions to those prohibitions so care can be provided and paid for without the need for individual authorizations. In fact, Rep. Shays' proposal does not appear to explicitly require specific authorizations, which is confusing in light of the extensive authorization requirements contained in Section 103 of the proposal. We understand that Rep. Shays is considering making revisions to this section of the bill before introducing it.

We believe the intent of Rep. Shays is laudable -- to allow health plans and providers to use protected patient information for treatment, payment and other functions that support good care management. AHA supports that goal. However, we believe this approach may make it difficult for providers to determine when they do or do not need an authorization. This lack of clarity, combined with the strong sanctions contained in the proposal, could encourage providers to obtain many authorizations throughout the treatment process -- even when not implicitly required -- potentially affecting the timely delivery of care.

Preemption of state law

The AHA believes that a strong preemption of state law is critical to the successful implementation of federal confidentiality legislation. People today live, work and travel in a multi-state environment; they also receive health care without regard to state boundaries. The best way to protect patient information is to set uniform national standards -- standards that are enforced

through a strong federal law. This law must preempt all state laws with which it may conflict, regardless of whether those laws are weaker or stronger.

The AHA believes that some exceptions to the federal preemption are appropriate, such as in the area of public health. However, those exceptions should be specific and very clearly stated, as they are in the latest Bennett draft. Leaving in place, as the Jeffords bill does, any state law that comes under the public health or mental health category will require patients, providers, and health plans to comply with a wide variety of confusing and potentially conflicting requirements. The AHA supports the specificity with which the Shays bill outlines public health laws that are not pre-empted. While the language would allow exceptions for some specific public health reporting requirements, it does not broadly exempt all public health laws from preemption. However, we are concerned that the bill leaves in place all mental health laws. This is too broad, and, as stated above, carries the potential for confusion.

Definitions

The definitions section of Rep. Shays' bill does not recognize a growing necessity of today's integrated health care environment: the need to coordinate care across several different settings. It also omits many other functions that are central to ensuring quality care, like outcomes evaluation, risk and disease management, and case management. In the Jeffords bill these functions are summed up in the combined definitions of treatment, payment and health care operations. The Bennett proposal is even more descriptive of these critical functions. We believe

these concepts should each be captured in the definitions section of proposed legislation, and also should be included as exceptions to the prohibitions on use and disclosure.

Law enforcement

The issue of law enforcement use of protected patient information is not a focus of this hearing, but America's hospitals and health systems believe very strongly that it must be addressed.

We were deeply disappointed that the Secretary of Health and Human Services, in recommendations for privacy legislation that she released last fall, did not extend consistent federal privacy restrictions to law enforcement agencies. Were legislation to be based on her recommendations, law enforcement agencies would have unrestricted access to confidential patient records, with only minimal involvement by a neutral court of law. In addition, these agencies would have potential free rein to disclose the information contained in the records they obtained. This is unjustifiable.

Current state laws may or may not impose appropriate restrictions on law enforcement agencies' access to patients' records. In states where appropriate restrictions do not exist, a patient's records could be subject to unrestricted access and use by law enforcement agencies.

Sen. Bennett's, Sen. Jefford's and Rep. Shays' bills all limit access to protected health information by law enforcement officials, and are significant improvements over the Secretary's recommendations. We are still evaluating the "probable cause" standard in the Jeffords bill, and

the standard in the Shays bill that weighs the needs of the investigation versus the need t › protect individuals' privacy.

In any case, the AHA strongly believes that protected health information should be available to law enforcement agencies only after a request has been made through a process that involves a neutral magistrate.

Hospitals and health systems have a long history of working well with law enforcement agencies We understand there are times when law enforcement agencies have a legitimate need for protected health information But law enforcement agents should not have greater access to this information than the patients themselves, and those who provide their health care.

Conclusion

Mr Chairman, the AHA applauds Rep Shays and all senators and representatives who have turned their attention to this critical issue and are working to put together much-needed national legislation. We share their goal of protecting the confidentiality of the patients we serve, while also ensuring that the free flow of information is not hindered.

As our nation's health care system becomes more integrated and more reliant on the exchange of information, national legislation to protect confidentiality can't come too soon But, as always, our main concern is with our patients We look forward to working with this subcommittee to

ensure the passage of federal legislation that protects patient confidentiality, promotes the efficient delivery of high-quality health care, and is truly a uniform national standard.

###

Mr. HORN. Well, thank you very much. That's a rather to-the-point statement, and I think you've covered some interesting issues here which we'll get into with all of your colleagues.

We now have Dr. David Korn, the senior vice president for the Division of Biomedical and Health Sciences Research for the Association of American Medical Colleges. Dr. Korn.

Dr. KORN. Thank you, Mr. Chairman.

I might mention that I assumed my present position at the association in September 1997, when I became vice president and dean of medicine, and professor of pathology at Stanford emeritus, where I essentially have spent my entire academic life of close to 30 years.

I'd like to express the association's appreciation to the subcommittee and to the members and staffs of both Houses of Congress for their efforts in trying to draft comprehensive medical privacy legislation. I'm particularly grateful to the extreme hospitality and willingness of staff members with whom we've interacted to explore these very, very difficult and complicated issues, to seek input from all sides of the debate, and most importantly, I think, for their patience, which has been remarkable.

Mr. Chairman, all of us are citizens, consumers, and patients, and we all share concerns about the apparent erosion of individuals' privacy in our contemporary society. Our members engage in medical and scientific education. They carry out the bulk of the Nation's biomedical research, and they deliver a very large amount of patient care delivery. We care about the full range of issues that are covered in these various bills and draft bills that have been proposed to date.

But let me take my time here to talk just a little bit about medical research, since others will talk about other factors.

In particular, I'd like to talk about what's often called secondary or retrospective noninterventional research which does not generally involve interactions with patients, but does depend on access to patient records and other related patient materials, like blood samples or tissue samples that accrue during the course of medical care.

Every major hospital, but particularly, the major teaching hospitals in our academic medical centers, has enormous archives of these materials that may go back for more than 100 or 150 years. They are a record of the expression of human disease over generations, how they behave, where they arise, where they go, how different efforts at therapy, diagnosis, prevention have failed or succeeded over this very long period of time. You might think about these records as being equivalent to the research contents of the Library of Congress. They're essentially indestructible and immortal, and they are there as a source of knowledge to be explored by investigators, when knowledge signifies a new direction or when there may be a new technology that makes it possible to go back into these stored materials and ask new kinds of questions, to gain new insights about the manifestations and behavior of human disease. That's how medical knowledge has been built.

When you and I go to a physician, we expect that physician to give us advice based on the best contemporary information available about what our particular problems may be, what kinds of

therapeutic modalities to recommend to us, to tell us what might work and what might not work. That knowledge has not been given to us on Mount Sinai. That knowledge has been patiently created over literally generations and hundreds of years back to the Middle-Ages, when Italian physicians during the Renaissance began doing autopsies on some of the patients that they had who died. Not because they had magical therapies or diagnostic acumen at that time, but simply because of this desire to learn, to know what happened. What can we learn from this experience that will give us better capability to deal with our living patients and patients that will come in the future?

Now having said all of that, the AMC has taken a very strong position that the nature of retrospective research; that is, not knowing at the time a patient is encountered, what questions, what technologies may be applicable to the disease of that individual in future years—is such that there really isn't any way to get a truly knowledgeable informed consent, because you don't know what questions you want the patient to agree to let you do. So, we've been leery of efforts to deal with the access to records for medical research through any kind of elaborate construction of consent provisions or other barriers, as we see them, to this access to the materials.

Rather, we prefer the approach of building very, very strong requirements for protecting the security of those data, as many of the current bills that have been proposed do. That is, there are institutional requirements for physical, administrative, and technical safeguards that have to be implemented; that there must be confidentiality policies that are clear and that carry penalties; and that there are criminal, civil, and often administrative penalties for intentional or negligent violation.

With such a structure of protection of the medical research data base, we believe that access to information that is not protected health information; that is, information that does not directly identify individuals, should really be pretty much without oversight or without IRB-required approvals as a matter of fact, as long as it's being conducted in institutions that meet Federal standards of security as I have described.

The issue of access to protected health information or individually identified health information is a very, very difficult issue. There are many investigators—and I know my colleague, Dr. Elizabeth Andrews, may speak to this—there are many investigators who can argue persuasively and do, that they need access to individually identified medical information for the purposes of their research project. Most of us need linkage; that is, we have to be able to know that a record or a sample or a record 5 years later will belong to the same individual with the disease that happens to be the subject of the study.

Most of us do not need names, but we do need an identifier system that provides linkage. Some people argue that they actually must have names in order to do their research, and I, more or less, agree with Ms. Goldman's comments that there is in the IRB system and in the Federal guidelines, provision for IRB's to access that need and to determine whether, in fact, it is legitimate, and if so, to grant permission to the investigators to proceed.

We think the IRB system has worked extremely well. We believe that putting an equivalent kind of process in place, in noncommon rule institutions as, I believe, both Mr. Shays' bill and the current version of the Bennett bill would do, is exactly the right approach. We think that with those provisions in place one should focus more on the creation of security systems and less on interminable debates about how to get at the consent issue. We just don't think the consent issue is the way to go on this.

I look forward to the discussions that will follow. And I thank you for this opportunity.

[The prepared statement of Dr. Korn follows:]

Mr. Chairman and members of the Subcommittee, I am David Korn, M.D., Senior Vice President for Biomedical and Health Sciences Research at the Association of American Medical Colleges (AAMC). I assumed this position on September 1, 1997, when I became Vice President and Dean of Medicine and Professor of Pathology, Emeritus, at Stanford University, where I had been on the faculty for 29 years. The AAMC represents the nation's 125 accredited medical schools, nearly 400 major teaching hospitals, more than 87,000 faculty in 89 professional and scientific societies, and the nation's 67,000 medical students and 102,000 residents.

The AAMC strongly supports the general intent of current Congressional efforts to strengthen the protection of individuals' personally identified health information from inappropriate and harmful misuse that can lead to discrimination or stigmatization. This intent is presently expressed in several bills in both Houses, including Senator James Jeffords' "Health Care Personal Information Nondisclosure Act," S. 1921, Senator Robert Bennett's discussion draft bill entitled "Medical Information Protection Act," and Representative Chris Shays' discussion draft bill entitled "Consumer Protection and Medical Record Confidentiality Act."

The AAMC is pleased that while according individuals a right of "confidentiality" of their individually identifiable health information and records, Representative Shays and Senators Jeffords and Bennett recognize that individual claims to "privacy" cannot be absolute in contemporary society. Rather, they must be tempered in a limited number of specific instances where public well being and responsibility require access to individuals' health information.

Indeed, the central challenge in any effort to protect the confidentiality of personal health information is to find the right balance point between the competing goods of individual privacy and the considerable public benefit that accrues from controlled access to health information for purposes of delivering medical care and conducting medical research.

Confidentiality legislation must acknowledge the compelling public interest in continuing to ensure access to patient records and other archival materials required to pursue biomedical, behavioral and health services research. Medicine has always been, and largely remains to this day, an empirical discipline, and the history of medical progress has been created over many centuries from the careful, systematic study of normal and diseased individuals. From those studies has emerged our present level of understanding of the definition, patterns of expression and natural history of human diseases, and their responses to ever improving strategies of diagnosis, treatment and prevention. Using archival patient materials, that is, medical records and human tissue samples obtained during the course of routine medical care, researchers have been able to gain powerful insights into the nature, epidemiology, therapy and prognosis of major disorders of high prevalence, great human suffering and enormous societal costs. Similarly, epidemiological and health services researchers have been able to access these archival materials to collect the large, appropriately structured and unbiased population samples required to generate meaningful conclusions regarding the incidence and expression of diseases in specified populations, the beneficial and adverse outcomes of particular therapies, and the medical effectiveness and economic efficiency of health care system operations. A vast amount of

important medical research remains to this day exquisitely dependent upon the continuing, ready accessibility of archived patient materials that have been accumulated over generations in the course of delivering medical care. Indeed, in the present climate of major public concern about the costs, quality and efficiency of our rapidly changing health care delivery system, the need to support and promote such retrospective epidemiological and health services research has become an urgent public priority.

The AAMC strongly believes that in attempting to deal with the difficult issues of medical information privacy, giving due recognition to both the complexity of our contemporary system of health care delivery and financing and the public benefits of medical research, the most feasible -- and in the long term, most effective -- approach is ***not*** to try to erect costly and burdensome new barriers to accessing medical information required to sustain these activities. Rather, legislative efforts should be directed, as most of the current proposals attempt to do, toward requiring the establishment of strong administrative, technical and physical safeguards to protect the confidentiality, security, accuracy and integrity of the classes of health information that are to be protected. Included among these safeguards should be strong institutional policies of confidentiality, which might appropriately meet federal standards to be developed. To complete the "security package," the bills should – and do – specify stiff criminal, civil and administrative penalties for intentional or negligent actions that violate medical information privacy. With stringent security requirements of this kind in place, the AAMC believes that legislation should refrain from attempting to construct elaborate barriers to the relatively unimpeded flow of medical

information that is required for both the effective delivery of health care and the promotion of a comprehensive national agenda of medical research.

Given the substantial penalties contained in the confidentiality bills now in draft or under consideration, including those of Senators Jeffords and Bennett and Representative Shays, it is imperative that the bills' definitions be crafted with great care and clarity. A common pitfall in many of the proposed confidentiality bills is their lack of sufficient precision in defining the class of medical information that is to be circumscribed for statutory protection. Of particular importance then is the definition of "individually identifiable health information," the class of information most in need of protection from inappropriate disclosure and harmful misuse, and correspondingly, of "non-individually identifiable health information," the class that would fall outside of the requirements of the legislation. Some of the bills, in framing their definition of protected health information, add to unambiguous terms like "information that directly identifies an individual" such additional phrases as "information that may reasonably be used to identify an individual" or "individually identifiable information" without further specification. These kinds of terms are highly subjective and open to a variety of interpretations, which makes them controversial. The AAMC believes that the protected class of medical information should be sharply circumscribed and limited to "information that directly identifies an individual." Such a definition is least ambiguous and strikes to the heart of the information that the public is most concerned to protect.

Correspondingly, the definition of "nonidentifiable health information" should encompass "information that does not directly reveal the identify of an individual." The definition should explicitly include coded or encrypted information (sometimes called "anonymized"), whether or not the information is linkable to individuals, as long as the encryption keys are secured and kept separate from the encrypted information itself. The justification for including encrypted, linkable information in the definition of nonidentifiable health information is significantly strengthened by adding the additional provision that makes it a crime to attempt to use encrypted patient data to discover an individual's identity by any means other than the lawful use of an encryption key.

The AAMC believes that a set of properly constructed definitions of individually identifiable and nonidentifiable health information will serve both to foster medical research and establish an incentive system for using nonidentifiable health information in such research to the maximum extent practical. Thus, under the definitions of individually identifiable and nonidentifiable health information favored by the AAMC, the burdens of enhanced security protections and detailed patient authorizations mandated in the Jeffords, Bennett and Shays bills would not be applicable to retrospective, non-interventional studies of archival patient materials using encrypted linkable data. Researchers would therefore be strongly encouraged to utilize encrypted data whenever the objectives of their research projects would not be compromised.

The intense concern of the AAMC with the definition of the classes of medical information to be protected by or excluded from the proposed legislation derives from the fact the precision of

those definitions will significantly determine the effect of any new legislation on medical research. We are especially concerned with the potential impact on what is commonly referred to as secondary research, that is, retrospective non-interventional studies of archival patient records or tissue samples. Such studies, although typically never requiring knowledge of individual patient identities per se, do as a rule require that the individual research materials be linkable both horizontally and longitudinally over time. That is, the investigator of disease must be able to link a given patient's tissue samples with her/his corresponding medical records, or to link the temporally or geographically separate medical records of specific patients to follow the course of particular disease processes and their responses to therapy. The very same requirements for linkage apply to large-scale population-based studies conducted by epidemiologists, health service researchers, and those who study strategies of promoting health and preventing disease in large populations.

For this reason, we are very concerned with any proposed definition of protected health information that uses ambiguous descriptors like "reasonably identifiable" or "individually identifiable" that could be construed to embrace linkable encrypted medical information. All of the proposed bills would require specific and detailed authorization for each instance of disclosure of protected health information, except in specified circumstances defined as "exceptions," which largely pertain to medical treatment, payment, health system operations, public health requirements and the needs of the legal system. To construe encrypted linkable medical information as "protected health information," and thereby to require specific and detailed

authorization for each access to that information would be not only exceedingly burdensome but chilling to the conduct of secondary research on archival patient materials.

These studies utilize patient records as primary research materials and do not involve any interaction with individual patients. Archival materials have been accumulating in academic medical centers for generations and constitute an enduring record of the expressions of human diseases, and the successes and failures of therapeutic interventions, over time. The materials represent a unique research resource and collectively constitute a "national archive"; they are essentially immortal, like the contents of the Library of Congress, for example, and that very fact defines much of their research value. It is veritably impossible at the time of encounter with an individual patient to predict -- or attempt to describe to the patient -- the particular types of research questions, methodologies or particular studies for which these materials might prove valuable in future years to deepen understanding of human disease.

In contrast to the typical interventional clinical research study, in which researchers directly interact with patients in well-defined clinical protocols and can provide them the detailed information required for informed consent, the uncertainties and unpredictability of secondary research make the applicability of the traditional informed consent procedure problematic. Accordingly, under the provisions of the Common Rule, such retrospective research has been singled out for special attention and, under the criterion that the proposed research may be deemed to be of no more than minimal risk to the research subjects, has typically been handled by

Institutional Review Bodies (IRBs) by waiver of review or use of the expedited review mechanism. The AAMC urges that any new medical information privacy legislation should take care not to introduce unnecessary and perhaps unintended, obstacles to secondary research on archival patient materials. The Association believes that for secondary research on encrypted, linkable patient records, conducted in organizations and under circumstances that meet statutory requirements for safeguarding the security of medical information, neither specific patient authorization nor IRB (or equivalent) notification should be required.

For secondary research on archival patient records that are individually identified, i.e., that fall within the definition of protected health information, the AAMC believes that a statutory requirement of specific authorization would be unwise and could seriously bias, and thereby undermine, the integrity of these vital research databases. Rather, the Association recommends that all such proposed research must be reviewed by an IRB or equivalent mechanism. The IRB would, in addition to satisfying itself about those matters currently specified in the Common Rule, be required to determine that (1) the organizational setting in which the research will be conducted is in conformity with statutory requirements for safeguarding medical information privacy; (2) the research requires the use of individually identified patient information and could not be performed without it; and (3) it would not be practicable or feasible for the investigators to attempt to obtain individual informed consent from the subject population. Such a review protocol, in the opinion of the AAMC, would sufficiently protect the privacy interests of research

bjects, while at the same time continuing to facilitate the conduct of a broad spectrum of
neficial secondary research on archival patient materials.

this regard, the Association opposes legislative language that would order IRBs to *weigh the
lue or significance* of proposed research and somehow *balance* that against the invasion of the
search subjects' privacy rights. Such a requirement would go well beyond the kinds of
sessment typically delegated to IRBs and would involve the introduction into the IRB review
ocess of value judgments about the importance of research that the Association believes would
highly idiosyncratic and inappropriate.

ıe AAMC strongly supports the argument that any new federal legislation dealing with medical
formation privacy be preemptive of state laws on this topic, with the exception of those dealing
ith public health reporting requirements, which are well established, time tested and closely
tegrated with the nationwide data collection and evaluation activities of the Centers for Disease
ontrol and Prevention. The Association recognizes that this recommendation is controversial,
ıt argues that the support of medical research is a long-established and high priority of the
deral government, and that there is therefore a compelling federal interest in ensuring that
edical research is facilitated, and not hindered or blocked by a discoordinated patchwork of
ırdensome state privacy legislation. Much contemporary medical research, especially
idemiological and health services research, requires access to large, unbiased population
mples encompassing many states. Accordingly, the Association recommends that any new

federal confidentiality legislation should over-ride state laws to ensure consistent nation-wide governance of access to archival patient materials for research. For this reason, the Association is troubled by the provisions in the Jeffords and Shays bills that would exempt from federal preemption state laws dealing with the protection of mental health information. While acknowledging the sensitivity of this issue, we point out that many different diseases are considered especially sensitive by those who suffer from them and their advocates, and to single out mental health information for special protection opens a loophole in the intended federal preemption that the AAMC believes would prove very difficult to limit.

The issues encompassed by concerns with medical information privacy are complex and difficult. We have constructed a health care system in this country that does not guarantee affordable access to quality care for all of our citizens. Accordingly, the risk of being denied access to affordable health insurance is real, and individuals are understandably concerned with safeguarding the security of and limiting access to their private and personal medical information. But the very complexity of our system of health care delivery and payment frustrates efforts to devise comprehensive and effective measures that would restrict access to medical information to the degree that the average citizen might desire. The AAMC believes that it is intrinsically possible to ensure a much greater level of protection for medical information created, maintained and used in the course of research than can be designed for medical information used in the course of providing medical care. Accordingly, the Association has recommended the erection of a fire-wall around human databases created in research that would make them nearly impregnable, and

offer them far more security from trespass than would be possible for clinical records used in health care delivery and payment.

The AAMC has earlier proposed that all entities conducting research on human subjects or archival patient materials, which have in place institutional policies and procedures that meet federal standards for safeguarding the confidentiality of medical information, should be eligible by some form of assurance mechanism to receive a federal protection modeled on the existing Certificate of Confidentiality. The protection would embrace all of an institution's human subjects research databases and shield them from forced disclosure of individually identified medical information to anyone, including family members, employers, insurers, health care organizations, or legal and judiciary processes. The Certificate of Confidentiality was created in 1970 to enable research projects on drug use patterns by Vietnam War combatants and veterans. It was incorporated into the Public Health Service Act in the mid-1970s, and was expanded in 1988 to embrace a wide range of research projects on human subjects, which generated sensitive or potentially stigmatizing information. To our knowledge, the confidentiality protections afforded by this certificate have never been breached, even though they were originally enacted to facilitate studies of activities and behaviors that were often criminal. The Association continues to urge that protections of institutional human research databases akin to those of the Certificate of Confidentiality be considered in crafting medical information privacy legislation.

The AAMC commends the Subcommittee for convening this hearing to address the need for confidentiality legislation, and the efforts of Senator Jeffords, Senator Bennett and Representative Shays to craft legislation that would enhance the security of medical records. The Association urges the Congress, as it wrestles with this difficult challenge, to be mindful of the fact that the facilitation of biomedical, epidemiological and health services research is a compelling public priority that has served this nation well and offers bright promise for the future of human health. The AAMC strongly believes that the combination of legislatively mandated safeguards of the security of individually identifiable medical information, stiff penalties for violations, and the creation of special protections of medical information that is created in research and maintained in research databases, as we have suggested, make it unnecessary to elaborate new, burdensome and potentially chilling restrictions of access to medical information for purposes of retrospective, non-interventional research.

Mr. HORN. We thank you for that very thorough statement and you've hit a few areas that we're going to have further discussion on.

Kathleen Frawley has a very distinguished background. She's a lawyer among other things, as well as a scientist, as well as a records administrator, and she's vice president of Legislative and Public Policy Services at the American Health Information Management Association.

Ms. FRAWLEY. Thank you, Congressman Horn. It's a pleasure to have the opportunity to appear before you again on the need for Federal preemptive legislation.

I do want to point out that I am a member of the National Committee on Violent Health Statistics, but the testimony I'll be offering this morning is on behalf of AHIMA, and does not reflect the committee's perspective on this issue.

As you know, the American Health Information Management Association is the professional association which was established in 1928. We have 38,000 members who work in healthcare settings throughout the United States, and are responsible for handling patient health information. Our members are responsible for handling release of information and making sure that this disclosure is pursuant to valid authorizations from the patient or subject to statute regulation or court order. This responsibility is not taken lightly and it certainly is complicated by the fact of lack of uniform national standards or guidelines.

Certainly, we've heard already from our witnesses that there has been increasing demands for data and that poses an ever-growing threat to patients privacy. It is important to note that currently there is no national standard for the confidentiality health information and that that protection is left to State law. As you indicated in your opening statement, we only have 28 States right now that allow patients access to their health information, and that is very problematic, and the fact that we are asking patients to authorize disclosure of their information and they often do not know what is contained in their health record.

If you look at the State statutes that we currently have, and that's certainly a major discussion when we talk about preemption, generally the patient access statutes that are on the record right now often talk about the fact that the patient may have access to their hospital records or sometimes their hospital records and physician records, but often do not address records maintained by third parties such as insurance companies or managed care plans.

And a lot of these statutes were enacted many years ago before the current complexity of our health care delivery system was contemplated. So, the existing statutes and regulations that our members work under are often not contemplating disclosures that are now ongoing in health care delivery systems.

Also, the other problem that we have with State law right now is protections vary according to the holder of the information, and vary, according to the types of information. Many statutes do not address redisclosure of health information which is very problematic for our members. The patient comes in, signs an authorization asking for information to be disclosed to a third party. Our members will send that information on and indicate to the recipient

they are prohibited from redisclosing that information. However, in many States there is no law, and therefore, we do know there are redisclosures and the fact that they are not contemplated or authorized by the patient.

And often these State statutes or regulations lack penalties for misuse or misappropriation of health information. Several States have recently enacted legislation to address the area of genetic privacy. In fact, there are 19 States that have done so. Again, the problem that you have is that if you look at these statutes they are not consistent in their approaches. And since we know that many of our citizens live on borders and across State lines to seek healthcare, that again, this is a problem.

We also have implications in the United States in the area of our global competitiveness. We do have the European Union directive which is effective October 1998, and certainly will affect our ability to compete in the global marketplace. EU directive recognized the need for harmonization among the member countries and certainly is an important area that we need to be concerned about.

As you know, AHIMA has had a strong tradition in this area. We held the first National Symposium on Confidentiality in July 1992 and had Arthur Ashe come forward and speak to us on the need for legislation in this area. He spoke very eloquently about his own personal 10-year battle with HIV and AIDS-related illnesses and his decision to go public. In 1993, AHIMA published a model code for health information which was the basis of Congressman Condit's Fair Health Information Practices Act which is pending before the subcommittee. We have had the pleasure of both working in the House and the Senate with many of staff and Members of Congress who are working on this issue.

We have had the opportunity to work with Congressman Shays on his draft and we think it's very important in terms of the fact that it addresses many of AHIMA's concerns regarding individual rights. And we believe that it is critically important, because many individuals have never seen their medical records. They have no idea who maintains their health information or for what purpose this information is used. So, we think this is very critical.

I will point out in support of the testimony of my colleague of the American Hospital Association that we need to be very careful though, that we understand that health information is used for a variety of purposes including patient care, quality assurance, education research, public health, and oversight functions. We think that's critical that any legislation before the Congress addresses all of these various issues. I would concur with his comments that the current language that Congressman Shays is offering may not be clear to everyone, in terms of what their expectations are and in terms of when authorization is required.

We think that the mechanisms in Congressman Shays' language, in terms of civil and criminal penalties is very important. And we also support the need for strong information security management programs, including policies and procedures to protect information.

I did serve as a member of the National Research Council which did an 18-month study on protecting electronic help information, and our report was released in 1997. It certainly has received a fair amount of attention. We believe that organizations, health care or-

ganizations and other recipients that have information need to do a better job of protecting patient information, whether it's paper-based or electronic-based.

The one concern that we do have with Congressman Shays' draft and also a number of bills that are presently under consideration is that it would not preempt State laws that regulate information about an individual's mental health or communicable disease status. We advocate—and I will tell you from personal experience—that comprehensive Federal preemptive legislation is required to ensure that there are uniform standards. All health information including genetic information should receive the same high-level of protection. Segregating creating special protections for specific types of information, whether it's mental health, communicable diseases, or genetic information, could result in inadvertent breaches of confidentiality by requiring different standards for the handling of that information.

It is imperative that strong Federal legislation that would prohibit any misuse of individually identifiable health information be enacted. We believe it's critical for Federal preemptive legislation to be enacted in this Congress and I thank you for the opportunity to present our comments.

[The prepared statement of Ms. Frawley follows:]

Mr. Chairman and Members of the Subcommittee:

The American Health Information Management Association (AHIMA) appreciates the opportunity to submit this testimony to the Subcommittee on Government Management, Information and Technology on the need for federal pre-emptive legislation to protect the confidentiality of individually-identifiable health information. AHIMA commends both Congressman Condit and Congressman Shays for their efforts in this area.

The American Health Information Management Association (AHIMA) is the professional association which represents over 38,000 credentialed specialists who, on a daily basis, manage and protect the health information that is an increasingly important component of our nation's health care delivery system.

AHIMA members work in health care organizations throughout the United States and ensure that an individual's right to privacy is protected. Health information management professionals handle requests for health information from third party payers, employers, researchers, attorneys, other health care providers and local, state and federal agencies. Our members ensure that information is disclosed pursuant to valid authorizations from the patient or their legal representative, or pursuant to statute, regulation or court order. This responsibility is not taken lightly and is complicated by the lack of uniform national guidelines or legislation.

For the past 70 years, AHIMA and its members have assumed the responsibility for protecting the confidentiality of health information. Our efforts have been complicated by the lack of federal preemptive legislation.

The primary goal of confidentiality is to allow patients to communicate with their physician and to share information regarding their health status. Trust is an essential element in the relationship between patients and health care providers. One of the most important aspects of this relationship is the provider's duty to maintain the confidentiality of health information. The historical origin of a physician's obligation, for example, is found in the Oath of Hippocrates, written between the sixth century B. C. and the first century A. D. The Oath states "what I may see or hear in the course of treatment in regard to the life of men, which on no account must spread abroad, I will keep to myself....." Ethical codes promulgated by associations of health care professionals have consistently recognized the importance of confidentiality. However, these codes do not address current issues regarding use and disclosure of health information.

While communications between patients and physicians are privileged in most states, the protection of these laws is very narrow. The privilege only applies when physicians are testifying in court or in related proceedings. Many of these laws include significant restrictions that further limit the availability of the privilege. The physician-patient privilege offers no real protection to patients regarding the confidentiality of their health information.

Increasing demands for data pose a growing threat to the patient's right to privacy. The Federal Privacy Act of 1974 was designed to provide private citizens some control over the information collected about them by the federal government. Health care facilities operated by the federal government, such as the Indian Health Service, Veterans Administration and Department of Defense, are bound by the Act's requirements regarding access, use and disclosure of health information. However, the provisions of this law do not apply to health information maintained in the private sector.

Federal alcohol and drug abuse regulations only apply to federal or federally funded facilities that offer treatment for alcohol or drug abuse. While these regulations offer strong protection, they are limited in applicability. Currently, there is no uniform national standard protecting the confidentiality of health information. The protection of health information is left to state law.

Currently, only 28 states allow patients access to their health information. However, these statutes are not uniform in their approaches. A review of these statutes reveals that in some states patients may only access hospital records, while in other states they may access both hospital and physician records. There is little uniformity among state statutes and regulations regarding confidentiality of health information.

Protections vary according to the holder of the information and vary for different types of information. Most statutes do not address redisclosure of health information and lack penalties for misuse or misappropriation. Several states have recently enacted

legislation to address issues regarding genetic privacy. However, there is no uniformity in their approaches.

It has been recognized that there is a need for more uniformity among the 50 states. In the 1980s, the National Conference of Commissioners on Uniform State Laws developed the Uniform Health Care Information Act in an attempt to stimulate uniformity among states on health care information management issues. Presently, only two states, Montana and Washington have enacted this model legislation. Clearly, efforts must be directed toward developing national standards on privacy and confidentiality.

THE NEED FOR FEDERAL LEGISLATION

Over the past several years, a consensus has emerged within Congress and among the general public regarding the need for federal legislation to address this important issue. The Office of Technology Assessment (OTA) report, Protecting Privacy in Computerized Medical Information, found that current laws, in general, do not provide consistent, comprehensive protection of health information confidentiality. Focusing on the impact of computer technology, the report concluded that computerization reduces some concerns about privacy of health information while increasing others. The OTA report highlights the need for enactment of a comprehensive federal privacy law.

In 1994, the Institute of Medicine released a report, Health Data in the Information Age: Use, Disclosure and Privacy, which recommends that federal preemptive legislation

be enacted to establish uniform requirements for the preservation of confidentiality and protection of privacy rights for health data about individuals.

In the final Office of Technology Assessment (OTA) report, Bringing Health Care Online: The Role of Information Technologies, the issues of privacy and confidentiality were identified as particularly important areas in dealing with health information. The report noted that if there is little confidence that an electronic medical information system will protect them, then providers and patients will be unwilling to use it. The report recommends that Congress establish federal legislation and regulation with regard to privacy and confidentiality of medical information, as well as storage media for medical records and electronic data standards for storage and transmission of medical information.

As a result of the ongoing public policy debate, The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) required the Secretary of Health and Human Services to submit detailed recommendations on standards with respect to the privacy of individually identifiable health information to the Congress. On September 11, 1997, in testimony before the Senate Labor and Human Resources Committee, the Secretary outlined her recommendations regarding the rights that an individual who is a subject of individually identifiable health information should have, the procedures that should be established for the exercise of such rights and the uses and disclosures of such information that should be authorized or required.

Under the Health Insurance Portability and Accountability Act, if legislation governing standards with respect to the privacy of individually identifiable health information is not enacted by August 1999, the Secretary of Health and Human Services is required to promulgate final regulations containing such standards by February 2000.

Additionally, there are implications for the United States as a result of the new European Union Data Privacy Directive and related policy and legal changes. In October 1995, the European Union adopted a "Directive on the Protection of Individuals with regard to the Processing of Personal Data and on Free Movement of Such Data". By October 1998, all 15 E. U. member states must bring their national laws into congruence with the directive. This directive applies to health data as well as to many other kinds of data.

On May 14, Vice-President Al Gore announced the "Electronic Bill of Rights" to help ensure the privacy of consumers' medical records, Internet transactions and other computerized personal data. The Administration is encouraging Congress to pass strict medical records legislation to how and when individuals' medical records can be used; give individuals that chance to correct those records; and give patients the right to be informed about them.

HEALTH CARE AND THE INFORMATION AGE

The development of the national information infrastructure (NII) is a key component of health care reform. Efforts to reform this country's health care delivery system will rely heavily on administrative simplification and computerization of health information to control costs, improve quality of care, and increase efficiency. The Institute of Medicine (IOM) report, The Computer- Based Patient Record: An Essential Technology for Health Care, recommended the adoption of computer-based patient records by the year 2000 and the formation of a nationwide health information network. However, as that report noted, there are states that require medical records to be written and signed. In order to facilitate the development of a national health information infrastructure, it is imperative that health information can be created, authenticated, and retained in electronic form.

Currently, the expanding use of information technology in health care raises questions about the ability of health-related organizations to ensure the security of health information and to protect the privacy of their patients. In March 1997, the Computer Science and Telecommunications Board of the National Research Council released a report, For the Record: Protecting Electronic Health Information. The report recommends that all organizations that handle individually identifiable health information adopt a set of technical and organizational policies, practices, and procedures to protect such information. It was noted that "adoption of these practices should help organizations meet the standards to be promulgated by the Secretary of Health and Human Services in

connection with the requirements of the Health Insurance Portability and Accountability Act".

The report also outlines possible legislative options for addressing systemic concerns:

- Legislation to restrict access to patient-identifiable health information based on intended use
- Legislation to prohibit specific practices of concern to patients
- Legislation to establish information rights for patients
- Legislation to enable a health privacy ombudsman to take legal action

The report notes that passage of the Health Insurance Portability and Accountability Act is "a first step toward giving patients greater ability to protect their health information but efforts to extend the fair information practices requirements of the Privacy Act of 1974 to the private sector would empower the consumer population with enforceable rights and create a powerful force for protecting the privacy and security of sensitive information".

To meet today's information requirements, the nation must move towards a health information infrastructure that will support computer-based patient record systems that capture clinical information, integrate it with clinical support and knowledge bases, and make it available for legitimate users.

Because health information remains largely uncomputerized and unintegrated, patient information is often inaccessible at the time health care decisions are made. Highly trained health care professionals spend valuable time looking for records, contacting each other to obtain basic information, and struggling to decipher handwritten entries or repeating tests because previous results could not be found or obtained quickly enough. National studies have estimated that health care providers spend on average approximately 40 percent of their time on paperwork. External users of health information, such as payers, researchers, governmental agencies, and others must depend on a limited set of data that often is not transmitted electronically, or sort through volumes of records for key information about an encounter.

A number of benefits can be achieved through widespread use of computer-based patient record systems. Health care providers would have more complete information about the patient instantly and easily. Care would be improved through the ability to access knowledge databases and online expert systems. Information systems would reduce the enormous paperwork burden that providers currently experience. Aggregate data from these medical records will enable better research.

One of the major prerequisites to the appropriate implementation of the computer-based patient record is the need for federal preemptive legislation to protect the confidentiality of health information. In order to move health care delivery systems into the 21st century, AHIMA believes that the nation cannot wait any longer to enact federal

preemptive confidentiality legislation. It is critical, and arguably, the most important aspect of any health care reform effort.

AHIMA'S POSITION

In February 1993, in order to address the need for federal legislation, AHIMA drafted model legislative language that outlined a code of fair information practices. This language was published in the OTA report, Protecting Privacy in Computerized Medical Information, as a model code. The language was also used by Congressman Gary Condit in drafting HR 52, the "Fair Health Information Practices Act" that is pending consideration before this Subcommittee.

There are a number of key provisions in AHIMA's model language that we believe are essential elements of any legislation to govern the collection, use, and disclosure of health care records. These include:

- **Disclosure** -- No person other than the patient or the patient's representative may disclose health care information to any other person without the patient's authorization, except as authorized.

  No person may disclose health care information except in accordance with the terms of the patient's authorization.

The provisions apply both to disclosures of health care information and to redisclosures of health care information by a person to whom health care information is disclosed.

- **Record of Disclosure** -- Each person maintaining health care information shall maintain a record of all external disclosures of health care information made by such person concerning each patient, and such record shall become part of the health care information concerning each patient. The record of each disclosure shall include the name, address and institutional affiliation, if any, of the person to whom the health care information is disclosed, the date and purpose of the disclosure and, to the extent practicable, a description of the information disclosed.

- **Patient's Authorization; Requirements for Validity** -- To be valid, a patient's authorization must:

    1. Identify the patient;
    2. Generally describe the health care information to be disclosed;
    3. Identify the person to whom the health care information is to be disclosed;
    4. Describe the purpose of this disclosure;
    5. Limit the length of time the patient's authorization will remain valid;
    6. Be given by one of the following means --

        a) In writing, dated, and signed by the patient or the patient's

representative; or

b) In electronic form, dated and authenticated by the patient or the patient's representative using a unique identifier.

The AHIMA model also includes the following principles of fair information practices:

- **Patient's right to know** -- The patient or the patient's representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purpose the health care information is used.

- **Restrictions on collection** -- Health care information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected.

- **Collection and use only for lawful purpose** -- Health care information must be collected and used only for a necessary and lawful purpose.

- **Notification to patient** -- Each person maintaining health care information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy

of the statement of a person's fair information practices and should receive an explanation of such fair information practices upon request.

- **Restriction on use for other purposes** -- Health care information may not be used for any purpose beyond the purpose for which the health care information is collected, except as otherwise provided.

- **Right to access** -- The patient or the patient's representative may have access to health care information concerning the patient, has the right to have a copy of such health care information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such health care information of any amendment or correction of such health care information requested by the patient or patient representative.

- **Required safeguards** -- Any person maintaining, using or disseminating health care information shall implement reasonable safeguards for the security of the health care information and its storage, processing, and transmission, whether in electronic or other form.

- **Additional protections** -- Methods to ensure the accuracy, reliability, relevance, completeness and timeliness of the health care information should be instituted. If advisable, additional safeguards for highly sensitive health care information should be provided. The AHIMA model language also contains

provisions for civil and criminal penalties to protect against unauthorized use or disclosure.

CONSUMER PROTECTION AND MEDICAL RECORD CONFIDENTIALITY ACT OF 1998

AHIMA is pleased to have the opportunity to work with Congressman Shays and his staff in the drafting of the "Consumer Protection and Medical Record Confidentiality Act of 1998". This bill contains many of the provisions based on the code of fair information practices contained in AHIMA's model language. We strongly support the concept that individuals have the right to know who maintains health information and for what purpose the information is used. Many Americans have never seen their personal health records and are unaware of the information contained in them.

Section 201, Inspection and Copying of Health Information, and Section 202, Amendment of Individually-Identifiable Health Information, will provide all individuals with the right to access their personal health information. These provisions also provide for the right of individuals to access their health information to amend errors if they do exist.

AHIMA strongly believes that individuals have the right to know who maintains their health information and for what purpose the information is used. Health care information is extremely personal and sensitive information, that if improperly used or

released, may cause significant harm to an individual's ability to obtain employment, education, insurance, credit, and other necessities. Health information concerning an individual must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected. There must be limitations on the use and disclosure of individually identifiable health information. The "Consumer Protection and Medical Record Confidentiality Act" addresses these issues in Title I, Restrictions on Use and Disclosure.

Health information is used for a variety of legitimate purposes, including patient care, quality assurance, education, research, public health, and legal and financial interests. It is critical that many of these activities which are required by federal and state statutes and regulations are addressed in this language.

We are pleased to note that the language is clear on the distinction between internal access to and use of health information by health care providers and external disclosure of health information. It is important that information flows within integrated health delivery systems and that no barriers are placed on providers who are trying to provide quality care to patients. There are many appropriate uses of health information within an organization and it is important to allow persons not involved in direct patient care to have access to carry out their responsibilities.

AHIMA strongly supports the need for mechanisms that will allow individuals to enforce their rights. We are pleased to note that Title III, addresses civil and criminal

sanctions. Additionally, we support the need for strong information security management programs, including policies and procedures, to protect information.

We are concerned, however, that the "Consumer Protection and Medical Record Confidentiality Act of 1998" would not preempt state laws that regulate information about and individual's mental health or communicable disease status. AHIMA advocates that comprehensive federal pre-emptive legislation is required to ensure that there are uniform national standards addressing the use and disclosure of individually identifiable health information.

All health information, including genetic information, should receive the same high level of protection. Segregating and creating special protections for specific types of information (i.e. mental health, communicable disease or genetic information) could result in inadvertent breaches of confidentiality by requiring different standards for the handling of this information. It is imperative that strong federal legislation that would prohibit any misuse of individually-identifiable health information be enacted.

SUMMARY

The movement of patients and their health care information across state lines, access to and exchange of health care information from automated data banks and networks, and the emergence of multi-state providers and payors creates a compelling need for federal law governing the use and disclosure of health care information.

AHIMA believes that it is critical for federal preemptive legislation to be enacted. AHIMA extends its thanks to the Subcommittee for holding this important hearing. We hope that this testimony will prove helpful to the Subcommittee. In addition to the points we have made here, we have additional technical comments which we would be pleased to offer as you continue work on the provisions of the "Consumer Protection and Medical Record Confidentiality Act".

Thank you for the opportunity to present our views. AHIMA looks forward to working with this Subcommittee and the Congress to enact legislation to ensure the confidentiality of individually identifiable health information.

Mr. HORN. We thank you very much for that helpful statement.

We now go to Dr. Richard Harding, who is a psychiatrist by background and vice president-elect of the American Psychiatric Association. You also serve on the National Committee on Vital and Health Statistics which was charged by Congress to make recommendations to the Secretary of Health and Human Services on protection of the confidentiality of medical records.

We're glad to have you here, Dr. Harding. Please proceed.

Dr. HARDING. Thank you, Mr. Chairman.

I am Richard Harding. I am a child psychiatrist from South Carolina and vice president-elect of the American Psychiatric Association. As my colleague, I sit on the National Committee on Vital and Health Statistics, but am not here representing that body, but the American Psychiatric Association and myself.

I'm grateful for the opportunity to appear before you, Chairman Horn, and would like to thank you as Chair, for the efforts supporting mental illness parity coverage and for the decision to hold these hearings. Positions are heartened by your actions and those of other officials, such as Vice President Gore calling for prompt action on medical record privacy. Prompt action is urgently needed.

We get into a difficult discussion because privacy is an elusive concept. It is defined as "the right to be left alone, to be free from scrutiny, tracking, surveillance, monitoring." The fundamental right to medical privacy has eroded in the last two decades. Traditionally, codes of ethics, Common law, and State statutes provided a high-level of patient confidentiality. As medicine goes from a cottage industry to a mega-industry however, new and mostly unregulated practices in the health care field, along with incredible advances in computerization of medical information have reduced the level of privacy, confidentiality, and trust in the system. Confidentiality is particularly essential in the treatment of mental illness including substance abuse.

The Supreme Court, in its 1996 decision involving the confidentiality of communications between a patient and a psychotherapist, ruled strongly in favor of confidentiality. The court said "because of the sensitive nature of mental illness, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment." It kind of speaks to the issue of stigma, prejudice, and discrimination that we face on a daily basis.

I urge the committee to ensure that the principle of privacy affirmed by the court in *Jaffee* v. *Redmond*, is contained throughout any medical record legislation that you approve. Otherwise, as the Massachusetts Medical Society has pointed out, the most aggressive Federal prosecutor may not be allowed to obtain the records of a psychiatrist, but a third party payer can routinely demand and receive full access to the most sensitive medical record. I would like to make four points before closing.

First, is that disclosure of medical information should be based on the informed, voluntary, and noncoerced consent of the patient. Patients must be allowed to say no to blanket consent without fear of losing their jobs or health insurance.

Second, Federal legislation should protect and encourage the confidential doctor-patient relationship. Physicians should continue their key role in the information disclosures process.

Third, Federal laws should not preempt State statutes or common law that protect patients medical information. Federal legislation should provide a floor of uniform protection for all individually identifiable medical information with States being allowed to continue to provide stronger privacy protection, if they deem it best for their citizens at the State level.

Fourth, as a fourth-generation physician, I am grateful for the technical advances that hold the promise of high quality care and improved public health. However, these same advances seem to stimulate an insatiable appetite for data among health systems. Their request to see the "complete medical record" cannot outweigh the patient's request for privacy.

We look forward to working with the committee in crafting legislation that will provide for a common good of our citizens while protecting their medical privacy rights. I again, thank you for this opportunity to testify.

[The prepared statement of Dr. Harding follows:]

Mr. Chairman, I am Richard Harding, MD testifying on behalf of the American Psychiatric Association (APA), a medical specialty society representing more than 42,000 psychiatric physicians nationwide. I am the Vice-President Elect of the American Psychiatric Association, and serve on the National Committee on Vital and Health Statistics which was charged by the Congress to make recommendations to the Secretary of Health and Human Services on protecting the confidentiality of medical records. The views I am presenting before the Committee today are my views and the views of the American Psychiatric Association.

I am grateful to have the opportunity to appear before you Chairman Horn, as well as Ranking Member Kucinich, and the other members of the Subcommittee. At the outset, let me thank you Mr. Chairman for your past efforts supporting mental illness parity coverage.

The American Psychiatric Association has consistently argued that federal legislation should not permit the disclosure of confidential information that identifies an individual without the individual's consent with the exception of narrowly-defined emergency circumstances and situations. We welcome the opportunity to work constructively with you on legislation that protect patients' right to privacy.

DOCTOR-PATIENT CONFIDENTIALITY IS CRITICAL TO PATIENTS' HEALTH

Confidentiality and trust between a physician and a patient are essential to successful treatment. Indeed, this relationship of trust is one of the key pillars upon which good medical practice is based. As the Hippocratic oath states, "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick...I will keep silence thereon, counting such things to be as sacred secrets."

In modern times physicians operate under an exacting standard of conduct developed by our profession. These professional rules are supported and strengthened by an extensive body of case law as well as statutes which provide additional legally enforceable confidentiality standards. Traditionally access to a patient's medical record is protected by a patient's physician or the physicians on hospital staffs exercising their strict judiciary duty to patients

Under these circumstances physicians, exercising their strict fiduciary duty to their patients, can protect patients' privacy and refuse inappropriate access. Physicians are also in a position to advise patients on tailoring voluntary disclosures of medical information so third parties can obtain the information they need without intruding on patient privacy. Patients can exercise informed consent to requests for disclosures, and they also have the ability to block virtually any disclosures of their medical records. Of course, much of these practices have now changed and many of the legal privacy protections are of limited use because they were crafted to provide privacy protections in the era before the rise of managed medical care and computerized medical records.

Clearly, confidentiality is critical to quality health care. Confidentiality can be a particularly important to the quality of care in cases of cancer and terminal illnesses, sexual function problems, and communicable diseases to mention just a few. If patients do not believe that what they tell their

doctor will not be widely disseminated many are unlikely to provide the full information necessary for effective treatment.

Nowhere is the need for confidentiality more clear than in the treatment of mental illness. As many medical experts point out: confidentiality is to mental health treatment what a sterile operating environment is to surgery -- a basic necessity for effective treatment. Often an individual seeks treatment because they are grappling with a highly personal and private issue: coping with the death of a loved one, the unraveling of family life, or feelings of depression and alienation. It would be difficult, if not impossible, for many patients to fully confront these issues unless they trusted the mental health professional and could be confident that the information would be kept private. For these reasons it is critically important to protect the confidentiality of patients' medical records.

In fact, in 1996 the U.S. Supreme Court recognized the critical importance of the confidentiality between patients' and mental health providers in its *Jaffee v. Redmond* decision. The Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust, and therefore the mere possibility of disclosure of confidential communications may impede development of the relationship necessary for successful treatment. The privilege also serves the public interest, since the mental health of the nation's citizenry, no less than its physical health is a public good of transcendent importance." We urge the Congress to recognize and accept the wisdom of the Court's decision and protect the confidentiality of the doctor-patient relationship.

THE EROSION OF PATIENT PRIVACY

But in the last twenty years, dramatic changes have occurred and are continuing to occur in the delivery of medical care and the use, transfer, and storage of medical records. New information technologies have grown explosively, and have been applied to medical practice in ways unforeseen even a few years ago. The growth of computerization and managed care has also increased the risk to patients of inappropriate and unnecessary disclosures of personal information.

Too many Americans are misled about how extensively their medical records are used and disclosed without their informed, voluntary, non-coerced consent. But gradually more Americans are learning that disclosures of medical records are occurring which can harm their privacy, compromise their personal life and their ability to obtain life or disability insurance, and their ability to find employment or earn a promotion. In addition, the lack of medical records privacy is likely to impact on outcomes research. Because patients fear that their information may not be kept private, they will be less likely to provide the full details of their medical condition. Thus because the underlying data was skewed the results of the research would not be as accurate as they would be in a system more protective of patient privacy. Finally, as more and more patients fill out detailed questionnaires from insurance companies about their health history that include information about their sexual experiences including any abortions, the quality of their relationships, and other sensitive personal issues the importance of the confidentiality of their records will increase.

Most of these disclosures occur because patients are not clearly informed of the uses of their personal health information and are not given a true opportunity to exercise voluntary, informed, non-coerced consent. In fact, third party payers are frequently demanding the entire medical record including even verbatim psychiatric notes containing the most intimate information about patients' lives. Such requests go far beyond what is legitimately necessary for these payers to perform their responsibilities. Likewise, the information that is required for treatment is often used for a host of additional purposes. In many cases, the individual records are used even though the technology exists to strip the medical records of patient identifiers. Thus, entire patient records are often accessible by thousands of individuals inside an organization and used by others for purposes other than treatment or payment.

Some of the additional uses of a patients' medical records are beneficial but particularly in these cases de-identified data should be used or the patient's consent secured. In many other cases, the medical record is being used against the patient's own interests. For example, life and disability insurance coverage companies may acquire this information and deny coverage to patients. And today these companies may deny coverage to a patient's family members who are "genetically" a higher insurance risk. In some instances medical information will be sold to direct marketers of health products without the specific informed consent of the patient.

If medical records are not adequately protected the impact on patients, particularly patients with mental illness, will be devastating. For example, the New England Journal of Medicine reported that a Maryland banker, by accessing medical records, determined which of his customers with loans had cancer. He then called in the loans. More recently a Florida public health office employee obtained computer access to 4,000 individuals who had tested HIV positive in confidential medical testing. The worker sent the names of these individuals to several newspapers in Florida.

Because psychiatric records more frequently contain sensitive personal information and because of the stigma that unfortunately still can be associated with psychiatric treatment, the consequences of the improper disclosure of these records is often very severe. In some cases following the disclosure of patient records the individual will stop seeking medical treatment. There have also been reported cases where co-workers learned the details of a colleague's mental health record and gossiped and joked about his problems. In this case the employer felt that the person's authority had been so undermined that the employer passed him over for a promotion.

To make the issue more immediate for members of the Congress, public officials and other prominent individuals are particularly vulnerable to improper disclosures of medical information. Several years ago the medical records including information on alcohol abuse problems of a Member of Congress from Arkansas were leaked to the press. This disclosure took its toll on voter support in the member's race for Governor, even though the information was subsequently shown to be false. And in 1992 it was revealed that one Member of Congress' medical records, including information about a suicide attempt, were splashed across the headlines of a major newspaper.

Because of these changes in the health care field and the resulting loss of privacy, new patient protections are needed. Without such action, Americans will not receive the quality health care and the privacy they deserve. We are very encouraged that Vice-President Al Gore, last week in his

address at New York University, focused public attention on the loss of personal privacy and suggested some additional action by the Clinton Administration on this issue. In particular we welcome his call for quick congressional action to protect the privacy of patient medical records.

PROVISIONS NEEDED IN FEDERAL LEGISLATION

The APA strongly supports the fundamental need for protecting medical records. We must have a system focused on protecting patients' privacy and their health. Physicians, in consultation with their patients, must be able to make key decisions concerning patients' treatment, health, and privacy. For all these reasons federal legislation should not undermine the time tested protections afforded by the doctor-patient relationship.

Federal legislation should protect personally identifiable information by ensuring that the following principles are contained in any legislation passed by the Congress:

- Federal legislation should protect and strengthen the doctor-patient confidential relationship. Physicians must be the key part of the information disclosure process in order to notify the patient of attempts to obtain private personal medical information or to inform the patient of potential consequences of disclosure.

- Patients' consent should be required before confidential information that identifies an individual can be disclosed, except in narrowly defined emergency circumstances. Physicians, patients, and other participants in the health care system need protections against the vulnerability of electronically transmitted information.

- Stronger state confidentiality statutes and federal and state common law should be preserved. Federal legislation should provide a "floor" of uniform protection for all personally identifiable medical record information. States should be allowed to continue what is essentially and historically a state's right: to provide stronger privacy protection for their citizens.

The APA is very encouraged by the bill, S. 1368, introduced by Senator Patrick Leahy (D-VT) and Senator Edward Kennedy (D-MA). This legislation contains several key provisions not found in any legislation now before the Congress. Patients are given basic rights to protect their medical information; most notably, they have the right to partition information in their records and with narrowly defined exceptions to control whether such information can be released, and are provided explicit notice of these rights. Equally important, under S. 1368, the federal law would provide a minimum acceptable floor to protect patient confidentiality, and thus any tougher or more restrictive state laws to protect that state's citizens would not be preempted. We urge the subcommittee to review the key privacy protections in the Leahy-Kennedy bill.

Numerous other medical records privacy bills have been introduced in the Congress. The APA is heartened that members of Congress are trying to address this urgent patient protection issue. Nevertheless, we do have concerns based on the principles outlined above.

These proposals do not yet provide the type of consent and revocation of consent provisions needed to protect patient privacy. For example, several bills would allow plans to terminate a patient's enrollment in a plan if they did not provide their full medical record to the plan for a wide range of uses other than for payment and their treatment. Likewise, patients are not afforded protections such as the ability to limit access to the most sensitive part of their medical record such as their mental health history or the verbatim psychiatric notes taken by their doctor. And finally, patients would not receive effective notice of their rights as well as the disclosure practices; some bills simply allow this information to be "posted" without any assurance the patient would receive this information.

Among our other major concerns are that stronger patient privacy protections are needed so that employers do not have inappropriate access to patient's medical records. We also believe that the most protective provisions possible are needed to prevent pharmacies from disclosing medications and other information without the specific informed consent of their patients. Important for all patients and particularly those wishing to receive treatment for mental illness are protections so that patients who wish to pay out of pocket can do so without divulging their sensitive medical information beyond their therapist. Finally, it is important to provide appropriate restrictions on the linkage of de-identified patient medical records with other computerized information, such as voter registration lists. (Such linkages can be performed for the purpose of re-identifying individual medical records).

In closing, let me reiterate the particular importance of protecting the confidentiality of the doctor/patient communication. Any interference with this relationship impairs the ability of a psychiatrist to help his or her patient and may cause the patient to stop receiving medical care. The APA urges the Subcommittee to accept what court after court has recognized as a legitimate zone of privacy - the psychiatrist/patient relationship - and protect the confidentiality of an individual's medical records.

We look forward to working with the Committee in crafting legislation that will provide the highest possible quality care and protect the privacy rights of patients. Thank you again for this opportunity to testify.

o:hard.tst

Mr. HORN. Well, we thank you, Dr. Harding. We appreciate you coming up here and as we get into this, I hope to get you all around the table going line-by-line after we paste up a few things in the next few months.

Our next presenter is Mr. Kahn. Mr. Kahn is the chief operating officer and president-elect of the Health Insurance Association of America. You might tell us a little bit about the association and who it represents and summarize your remarks.

Mr. KAHN. Thank you, Chairman Horn.

I am Chip Kahn, chief operating officer and president-designate of the Health Insurance Association of America. I appreciate the opportunity to present testimony today on behalf of our 250-member companies. I should add that until this January, I served as staff director to the Ways and Means Subcommittee on Health, where I helped draft many of the key provisions of the Health Insurance Portability and Accountability Act of 1996, HIPAA, including those relating to administrative simplification of health insurance claims and patient confidentiality.

The HIAA supports strong National standards to protect patient confidentiality. However, we also believe any new Federal requirement should be designed to protect consumers without imposing unnecessary complex, costly, or burdensome requirements that would excessively increase consumer premiums or other health care costs.

In today's complex and specialized health care systems, patients often obtain care from a variety of health care practitioners. By definition, appropriate, effective, quality care can be provided only through cooperation and sharing of medical and other health information. Accurate and readily available health information is vital to determining the best course of treatment for each patient. Health information is also critical to carrying out basic insurance functions, from paying claims to obtaining accreditation to preventing fraud and abuse.

The insurance industry believes it is critically important that consumers feel confident that access to health information by health care providers and payers does not mean unfettered access. That is why today, even in the absence of broad Federal requirements our companies ensure that sensitive information is kept confidential through a combination of voluntary practices and compliance with existing State and Federal laws. Legislation regarding the confidentiality of medical records represents both Congress and the health care industry with complex and difficult choices. We believe that the key to good public policy is to strike a careful balance between assuring confidentiality and maintaining accessibility to medical and health records.

But it can be accomplished, we think, if Congress follows five basic principles. HIAA member-companies believe the Federal legislation regulating the use, access, and disclosure of individually identifiable health information should: One, assure strong, uniform confidentiality protections for consumers while providing for equal treatment of health information, including genetic information and mental health information; facilitate appropriate uses of patient health information and recognize that access to health information is helpful to patients, both in providing quality care and conducting

nedical research; three, it should provide for uniformity of rules regarding health information through preemption of State law with appropriate exceptions for laws necessary to protect public health and safety; fourth, it should continue to recognize that access to, and use of medical information is important in antifraud efforts; and finally, provide fair penalties as a strong deterrent to the misuse of individually identifiable health information, rather than mandating costly bureaucratic administrative procedures for handling information.

In my written testimony submitted to the committee, I have elaborated on each of these points. The written testimony also provides extensive analysis of the impact on the private health care market of a draft legislation being considered by Representative Shays, the Consumer Protection and Medical Record Confidentiality Act.

In the time remaining, I would like to make a few general observations about the legislation proposed by Representative Shays.

First, Representative Shays' proposal is unique from other legislative initiatives because it provides a list of clear prohibitions and consequent penalties. Regardless of structure, the real key is whether legislation distinguishing between appropriate use and misuse of health information is clear and rational, and whether the rules are practical and do not impose regulatory burdens that unduly increase premiums costs for customers.

Based on the principles I've outlined, the HIAA believes that Representative Shays' proposal could provide a sound framework for establishing workable Federal rules for health information confidentiality. Second, the draft contains a good preemption provision. However, this section should be strengthened to treat all types of information in a uniform manner. It would free health insurers and managed care plans from costly and burdensome compliance with most forms of State-by-State regulation. Third, the legislation would allow consumers to limit the disclosure information by requiring providers of health plans, employers, and others to obtain individual authorizations before disclosing health information. Importantly, however, it would not be necessary to obtain individual authorizations to use health information for core functions such as billing and payment, quality assurance, and provision of health care.

In addition, the draft legislation provides for uniform national processes for obtaining authorizations where they're required. Finally, the legislation would impose penalties for the misuse of information rather than mandating burdensome bureaucratic processing for handling information.

At the same time we have concerns about certain key areas of the legislation on which we elaborate in our written testimony. For example, we believe that the broad carve out from Federal exemption for State mental health is unnecessary and could even inhibit quality care. In addition, the lack of materiality standard could subject physicians, providers, researchers, insurers, and employers the unwarranted liability including private civil action and criminal prosecution for mere technical violations of the act.

In closing, let me reiterate the importance of National uniformity in this area. Laws and regulations regarding the collection, use,

transmission, storage, and disclosure of health information reach to the heart of the insurance transactional process, and have a major impact on insurers core business and systems functions. These critical functions increasingly are carried out across State lines through the use of computerized data transaction systems. Without uniformity, health insurance premiums will increase with variations in compliance rules. And, high compliance costs resulting from State-by-State regulation would only exacerbate the already looming resource pressures insurers face in readying their systems for the year 2000.

Once again, I appreciate the opportunity to testify before you today on this important issue, and look forward to working with the subcommittee as you consider Federal legislation to protect patient confidentiality.

[The prepared statement of Mr. Kahn follows:]

I am Charles N. Kahn, Chief Operating Officer and President-designate of the Health Insurance Association of America (HIAA). I appreciate the opportunity to present testimony on behalf of our membership to the Government Management, Information, and Technology Subcommittee about medical records confidentiality. HIAA is the nation's leading advocate for the private, market-based health care system. Its 250-plus member companies provide health, long-term care, and disability-income coverage to more than 65 million Americans.

HIAA has a long history of excellence in representing companies that have had, and will continue to have, strict standards in place for protecting medical records. During the 104th and 105th Congresses, HIAA has been a vocal proponent of the need to protect individually identifiable health information. We have worked diligently at both the state and federal levels to make sure that confidentiality safeguards are in place that do not impede consumers' access to high-quality health care.

HEALTH INFORMATION IS THE LIFEBLOOD OF THE MODERN HEALTH CARE SYSTEM

The days of a patient seeing only a single family practitioner have ended. Today, patients obtain care from a diverse group of health care practitioners, such as specialists and allied health care professionals. Effective care, then, can only be provided through cooperation among practitioners who must share (and often communicate about) a patient's medical information

As our nation has moved increasingly toward a system of integrated care and computerized transactions, the free flow of medical information becomes even more critical. Accurate, readily available health information is vital to determining the best course of treatment for a patient, and that is clearly its central and most important use. Also critical is the use of such information to help ensure that basic insurance functions are carried out—from paying claims to preventing fraud and abuse. Finally, medical information is used for many other purposes: to assure health care quality, to help measure health outcomes, and to ensure that patients receive preventive services, to name only a few.

Insurance and managed care companies make responsible use of information; and they also have in place parameters that assure confidentiality. In addition, there exists a network of state laws that also protects sensitive medical information. We in the insurance industry understand that consumers must feel confident that access to health information by providers and payors does not mean unfettered access by the public at large.

LEGISLATIVE BACKGROUND

The "Health Insurance Portability and Accountability Act of 1996" (HIPAA) gives the Secretary of Health and Human Services (HHS) broad authority, with relatively little guidance, to promulgate binding regulations governing the use of individually identifiable health information if Congress fails to enact legislation in this area by August 1999. These rules, which could govern claims administration, enrollment and disenrollment processes, payment and remittance advice, referrals and authorization certifications, and other areas,

would have a significant impact on the day-to-day operations of every health insurance carrier in the United States. Because these regulations would coexist with existing and future state laws on patient confidentiality, they would by definition burden the industry with additional, duplicative, and, perhaps, conflicting administrative responsibilities. The end result would be an additional layer of bureaucracy and increased costs.

We already have had a preview of what the Administration would propose, if given the opportunity. Late last year, Secretary Shalala reported to Congress the Administration's recommendations for safeguarding the confidentiality of individually identifiable health information. Although the Secretary's statements at that time evidenced an appreciation for the necessary uses of health information within the broad context of health care delivery and research, the Administration's detailed legislative recommendations give rise to several very serious concerns. HIAA supports the general principles set forth by the Administration and shares its goal of achieving a balanced approach to ensuring the confidentiality of medical records. However, if the Secretary's recommendations were enacted into law or promulgated as regulations, they could jeopardize the ability of the health care industry to continue to promote high-quality, affordable health care services and coverage for consumers.

As Congress considers these recommendations and weighs its own response, it is critical that any new federal requirements not impose unnecessarily complex, costly, or burdensome requirements on the business operations of health insurers.

In addition to studying the Administration's recommendations, HIAA also has focused on the details of specific bills that are under consideration by the Congress. In this regard, much of our attention has focused on Senator Bennett's "Medical Information Confidentiality Act." Senator Bennett has brought to this issue a keen understanding of how the current health care system works and has attempted to accommodate these real-world exigencies into his initiative. Perhaps most important, Senator Bennett has been willing to consider recommendations from the health insurance industry and others as he continues to refine his approach to this issue.

In contrast, we have concerns about several features of Senator Jeffords' proposed legislation, the "Health Care Personal Information Nondisclosure Act of 1998." For example, the legislation contains a burdensome process for obtaining authorizations and carves out from its preemption provisions, without justification, all state laws related to mental health. It also includes several overly broad definitions that could have serious unintended consequences for the nation's health care delivery system.

HIAA'S BASIC PRINCIPLES WITH REGARD TO CONFIDENTIALITY LEGISLATION

Medical records confidentiality legislation presents the health care industry with hard choices and difficult tradeoffs. The importance of trust in the provider-patient relationship must be preserved. Health records are used to improve health care quality, reduce health care costs, expand the availability of health care services, protect public health, and assure

the accountability of the health care system. Confidentiality, when taken in its purest form-- by putting firewalls around information-- potentially undermines all of these objectives. Congress must strike a careful balance between assuring confidentiality and maintaining accessibility to medical records.

As Congress debates various legislative proposals in search of a workable federal legislative solution, we would like to reiterate the basic principles that underlie HIAA's support of federal standards governing patient health information confidentiality. We believe that any federal standards should:

- Provide equal treatment of all individually identifiable health information, including genetic information, to assure strong and uniform confidentiality protections;

- Facilitate appropriate use of patient health information and recognize that access to health information is helpful to patients and critical both to providing quality care and conducting medical research;

- Provide for preemption of state law, with appropriate exceptions for those laws necessary to protect public health and safety;

- Continue to recognize that access to and use of medical information is important to anti-fraud efforts; and

- Provide fair penalties as a strong deterrent to misuse of individually identifiable health information, rather than imposing process-oriented regulatory requirements.

Before we comment on the details of the draft legislative proposal by Representative Shays against the backdrop of these principles, we would first like to elaborate on each of these key points.

TREAT ALL IDENTIFIABLE HEALTH INFORMATION IN THE SAME MANNER

HIAA supports extending strong and consistent confidentiality protections to all individually identifiable patient health information. As such, HIAA is concerned about recent legislative proposals that would treat genetic information and mental health information separately from other health information-- either by providing heightened federal protections or carving out these areas from federal preemption.

It generally is in the best interest of patients for providers to have a complete and accurate picture of an individual's medical history. In many cases, quality care can only be assured by allowing providers to have access to a patient's complete medical record. Moreover, there are genetic components inherent in almost all health information. Therefore, it would be extremely difficult as a practical matter for health plans and providers to treat genetic information differently than other patient health information.

ALLOW FOR APPROPRIATE SHARING OF HEALTH INFORMATION TO ENSURE QUALITY

Today, most health care services are delivered through some form of coordinated or organized system of care. A 1997 KPMG Peat Marwick survey, for example, found that 82 percent of individuals receiving health benefits from their employers are part of a managed care plan. As health plans, physicians, hospitals, purchasers, and others in the health care market continue to design and enter into innovative health care delivery arrangements, it is important to recognize that appropriate information sharing and use must occur within that system to ensure that patients receive appropriate health care services.

The trend toward coordinated care offers greater opportunities to protect confidential patient health information, and to ensure that such information is used appropriately to benefit consumers. Some believe that coordination and computerization undermine confidentiality. In fact, sophisticated coordinated systems of care enable improved monitoring of health information and more meaningful protections to assure appropriate access to, and uses of, such information.

Any legislation relating to the confidentiality of health information must, by definition, distinguish between uses and disclosures that are "appropriate" and those that are "inappropriate." In making this legislative distinction, we urge Congress to exercise great caution. While it is important that patients have meaningful assurances of confidentiality,

legislation must not impede health system innovation that continues to enhance quality care.

FEDERAL STANDARDS AND PREEMPTION

Providing uniform national standards for confidentiality is the only way to avoid a dual regulatory structure for medical records. Federal standards that ensure the confidentiality of patient health information are critical to guaranteeing uniform and consistent treatment of such information throughout the country. At the same time, state authority should remain paramount with regard to areas that do not conflict with national uniformity and consistency, such as state reporting requirements for public health and safety.

While HIAA supports the enactment of federal confidentiality legislation, we note that assurances currently exist in the private market to protect patient health information. Most health plans and hospitals already have in place systems and procedures for ensuring patient confidentiality as a matter of professional practice, and as part of existing accreditation processes.

Laws and regulations governing the collection, use, transmission, and disclosure of health information reach to the heart of the insurance transactional process and have a major impact on insurers' core business and systems functions. These critical functions increasingly are carried out across state lines through the use of computerized data transaction systems.

Therefore, medical record confidentiality is an area of insurance law in which a significant degree of non-uniformity could impede the industry's ability to operate efficiently and meet the demands of its customers. The resources that must be devoted to compliance with differing state laws in this area can be significant. Adding a new layer of federal regulation without preemption of existing state confidentiality laws would only compound the difficulty. High compliance costs resulting from multiple duplicative or conflicting regulatory requirements would almost certainly be passed on to consumers in the form of higher health insurance premiums. Such cost pressures would exacerbate the already looming problem insurers face in readying their computer transaction systems for the year 2000. Moreover, dual state-federal regulation in this area would be directly contrary to the goals Congress set forth for administrative simplification in HIPAA—namely, a uniform set of national rules to simplify the health insurance claims process, reduce paperwork burdens, and reduce costs. Therefore, HIAA would support only those proposed federal laws that would preempt most state laws affecting the insurance industry.

DO NOT IMPEDE ANTI-FRAUD EFFORTS

Patient medical information is important to anti-fraud activities carried out both by the government and by insurers. A 1998 audit by the HHS Office of the Inspector General found that Medicare made improper payments of approximately $20 billion in fiscal year 1997 alone, and the General Accounting Office has estimated that health care fraud accounts for up to 10 percent of national health care spending each year.

Insurance information and patient information are the vehicles through which health care fraud is committed. Providers cannot falsify claims and medical equipment suppliers cannot submit inflated bills without access to patient information. At the same time, this information is critical to combating fraud, as investigators must depend heavily upon the use of medical records to document fraud cases. This does not necessarily mean that individually identifiable patient information must be publicly disclosed in order to successfully investigate and prosecute fraud. But it does mean that fraud investigators in both the public and private sectors must continue to have *access* to such information.

When developing federal legislation for confidentiality of health information, Congress should be mindful that overly prescriptive privacy protections may adversely affect health care fraud enforcement and ultimately be detrimental to consumers.

PROVIDE FAIR PENALTIES FOR IMPROPER USE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Although protections currently exist to protect patient confidentiality, there will always be those few who do not play by the rules. Those few should be punished.

Improper uses of patient health information should be prohibited. In fact, HIPAA expressly prohibits insurers offering coverage in connection with group health plans and self-insured employers from denying an individual health care coverage on the basis of health status. In addition, state and federal laws such as the "Americans with Disabilities

Act" and the "Civil Rights Act" already are in place to prohibit employment-based discrimination.

Again, the key to resolving this critical issue is balance. While consumers' concerns over the confidentiality of health information must be addressed, we must be careful not to adopt unduly restrictive legislation that undermines the ability of the health care industry to provide these same consumers with the high-quality, affordable health care services they deserve.

ANALYSIS OF REPRESENTATIVE SHAYS' PROPOSAL

We appreciate the opportunity today to comment specifically on the May 14 draft legislative proposal by Representative Shays, the "Consumer Protection and Medical Record Confidentiality Act," which has not yet been formally introduced. Our comments on Representative Shays' proposal reflect our extensive experience not only with other proposed federal legislation, but with the existing National Association of Insurance Commissioners' Insurance Information and Privacy Protection Model Act (the "Current NAIC Model Act") and with the deliberations currently taking place regarding the draft NAIC Health Information Privacy Act (the "Draft NAIC Model Act"), which is still under development. We would like to note for the record that HIAA has major concerns with the Draft NAIC Model Act as currently formulated.

General Observations

At the outset, we note that Representative Shays' proposal is based on a slightly different structural model than the Current NAIC Model, the Draft NAIC Model, the Administration's recommendations for protecting patient confidentiality, and the leading Senate bills. These other initiatives begin with the general proposition that all health information must be kept confidential, and then proceed to provide specific, legislative exceptions to that general rule. In contrast, the draft legislation proposed by Representative Shays provides a list of general prohibitions and consequent penalties.

While this structure holds promise, the real key from our perspective is whether the distinctions between allowable and inappropriate uses of health information are clear and rational, and whether the rules set forth in the legislation are workable or impose undue regulatory burdens on the private health care market.

Having reviewed the draft legislation in some detail, it appears that the proposal meets most of the important HIAA objectives outlined above. We believe that the proposal could provide a sound legislative framework for establishing workable federal rules for health information confidentiality. At the same time, we have significant concerns about several key areas of the legislation, which are outlined in greater detail below. Our comments extend only to those provisions where HIAA member companies have taken a position on reforms that may impact the health insurance industry.

TITLE I—RESTRICTIONS ON USE AND DISCLOSURE

Section 101. General Prohibitions and Exceptions

This section sets forth actions and inactions on the part of a person who discloses individually identifiable health information that are prohibited and constitute a violation of the Act. Prohibited conduct would include the following:

- Negligently or intentionally disclosing individually identifiable health information without an authorization or in a manner that is inconsistent with the terms of the authorization (Sec. 101(1)). We would strongly recommend introducing the concept of "materiality" into this section so that technical violations would not be subject to the civil, criminal, and programmatic penalties prescribed in Sections 301, 302, and 303 of the proposal. This concept is embodied in the Current NAIC Model Act and is consistent with the current position of the NAIC with regard to development of its Draft NAIC Model Act. The HIAA supports the exceptions provided in this section indicating that individual authorizations generally are not necessary for activities related to payment, the provision of health care, licensing and accreditation, and quality assurance. The burden of obtaining, or being unable to obtain, individual authorizations for disclosures in connection with these activities clearly would impede the core business functions of our member companies.

- Negligently or intentionally failing to provide for reasonable protections against disclosures of individually identifiable health information (Sec. 101(2)). The draft legislation would require health insurance carriers and others to develop and implement "reasonable and appropriate" safeguards to ensure the confidentiality of individually identifiable health information and to protect against certain threats to the security of such information. The draft legislation provides no specific definition or guidance as to what protections would be considered "reasonable" or "appropriate." On the one hand, this lack of specificity could allow carriers the flexibility to develop safeguards that are tailored to their own operational needs and the needs of their customers. On the other hand, the language may be interpreted to give regulators and the courts broad license to determine whether carrier practices are reasonable. We believe flexibility is important as carriers' internal operations can differ significantly. Therefore, if this type of language is retained, we urge you to clarify that discretion is intended to be utilized by the private sector rather than regulatory agencies.

- With respect to a person whose employees, agents or contractors come in contact with individually identifiable health information in the course of their employment, agency or contract execution, negligently or intentionally failing to establish written policies concerning compliance with the Act, including failing to establish procedures for monitoring access to individually identifiable health information (Sec. 101(3)). This language is similar to a provision being considered in the Draft NAIC Model Act and is of major concern to HIAA's members. At issue is the notion that carriers are

required to ensure that entities they contract with are in compliance with the Act. Our members are very concerned about the amount of administrative oversight that would be required on their part for ensuring that a contractor is in compliance with the Act, as well as the potential for holding carriers vicariously liable for actions of their contractors

- Negligently or intentionally failing to enter into a written contract with an agent, contractor or other person to whom individually identifiable health information is disclosed for a business purpose, prior to disclosure, specifying the limitations on their use and retention of such information and informing them of their responsibilities under this Act (Section 101(4)). HIAA's members generally are supportive of this type of notification requirement. However, we would strongly urge you to consider including language that specifically holds insurance carriers harmless for the actions of their agents and contractors, so as to avoid the implicit creation of liability by virtue of the duty to inform.

- Intentional disclosure of individually identifiable health information that constitutes a sale or commercial publication of the information (Sec. 101(9)). Based on the most current draft legislation, it appears that Representative Shays is undecided whether disclosure of health information for commercial purposes should be permitted, even with the individual's authorization (the reference to the exception contained in subsection (b)(2)(B) is in brackets, indicating that the exception may be eliminated). We caution here that both the terms "sale" and "commercial publication" may be

subject to overly broad interpretations which could hinder the ability of health insurers to carry out necessary business operations. For example, a carrier may contract for a fee with a group practice or disease management group to provide services for specific enrollees. Another example of a valid commercial use of health information would be sharing such information among affiliates, especially in a managed care setting, for the purpose of notifying enrollees of the availability of preventive programs or other health care services in which they may have an interest. While this type of activity clearly benefits enrollees, it technically could be prohibited by the legislative language in this section without further clarification.

Section 102. Special Rules for Anonymized Information

This section would, among other things, prescribe rules governing access to, and use of, health information in coded form, such as that provided to, and available from, the Medical Information Bureau (MIB). The MIB is a central computerized facility that keeps on file and makes available to HIAA member companies (in coded form and subject to strict confidentiality protections) health information pertaining to applicants for life and health insurance. Subsection (b)(2)(B) of this section would allow anonymized information to be "used" (e.g., obtained from the MIB) by an insurer with proper authorization, which normally is obtained when the individual applies for insurance. At this point, we have not been able to obtain a final legal opinion as to whether this section of the draft legislation would in any way impede the activities or current confidentiality protections of the MIB. As such, we ask that the Subcommittee provide us an opportunity in the near future to

comment more knowledgeably about the potential impact of this provision upon those activities.

Section 103. General Requirements for Authorization of Disclosure of Information

This provision sets forth the content of, and process for, obtaining an individual's authorization for disclosure of health information, where necessary. An authorization would be valid if it satisfies the federal requirements set forth in the draft legislation. HIAA believes that the requirements listed for obtaining a valid federal authorization generally are reasonable. We also support the flexibility which the provision would afford for our member companies-- particularly because so many of their day-to-day operations involving health information are carried out across state lines-- to utilize the uniform federal authorization standards, rather than comply with the potentially inconsistent laws of multiple states.

The draft legislation would require insurers to have in place "reasonable procedures" permitting individuals to revoke an authorization. We would be concerned both from an administrative and legal standpoint if an explicit requirement were included-- either through legislative language or by regulation-- that insurance carriers allow individuals an open-ended opportunity to revoke an authorization at any time. We therefore believe more clarification on this point could be useful in specifying the terms of a "reasonable" procedure for revocation.

Section 104. Disclosure in Civil Proceedings

This section prohibits a person from disclosing individually identifiable health information for use in civil proceedings in the absence of a valid discovery request, subpoena, or judicial order determining that the need for the information outweighs the individual's privacy interest. While we do not have a formal position with regard to this section at this time, we do note that its adoption could delay the discovery or pleading process in a broad array of civil proceedings and therefore could impede the ability of insurers to quickly resolve grievances and benefit coverage disputes. This is particularly true in the context of the Medicare program, where there are specific time frames required for resolving coverage disputes and grievances and against the backdrop of current legislative and regulatory proposals to extend similar time frames to the private market. The provision may also be interpreted to unduly restrict the use of health information in civil insurance fraud proceedings.

Section 105. Disclosure for Criminal Law Enforcement Purposes

This section is similar in construction to Section 104, but relates to disclosure of individually identifiable health information for criminal law enforcement purposes. Again, the HIAA does not have a formal position on this provision at this time as its potential implications are still under legal review. Consistent with the principles set forth earlier in our testimony, however, we would like to highlight the importance and valid use of health information as a tool for insurers to fight health care fraud. We caution Congress to carefully weigh the potential impact that section 105 may have on insurance fraud proceedings and investigations.

TITLE II—INDIVIDUALS' RIGHTS

Section 201. Inspection and Copying of Health Information

In general, this section would require providers, health plans, employers, health or life insurers, schools, and universities to inspect and copy their individually identifiable health information maintained by such entities. We note that the right of individuals to inspect and copy their health information in the possession of carriers, along with the ability of carriers to charge reasonable fees associated with such inspection and copying, is consistent with both the Current NAIC Model Act and the developing Draft NAIC Model Act, and the HIAA does not object to this provision. Again, we encourage Congress to provide as much flexibility as possible for carriers to make a realistic assessment of the cost associated with the burden of allowing inspection and copying of such records.

In addition, the exceptions to the inspection and copying rights specified by the draft legislation (endangerment to life or safety, identification of confidential sources, and information compiled in anticipation of litigation) are supported in concept by the industry. Finally, we support subsections (d), (e), and (f) of this section relating to the process for denial of requests for inspection or copying. We also welcome the reasonable limitations on this individual right relating to agents and hearings that are provided in subsections (g) and (h).

Section 202. Amendment of Individually Identifiable Health Information

The procedures set forth in the draft legislation for: (1) amending individually identifiable health information, (2) refusing to amend, and (3) filing a statement disagreeing with the refusal to amend are consistent with the Current NAIC Model Act. The rules governing agents in subsection (d) also are consistent with the Current NAIC Model Act. These procedures and rules generally are supported by HIAA members. We note, however, that subsection (a)(3), which would require insurance carriers and others to inform any individual or entity to whom unamended information was disclosed during the previous year of an amendment, could impose unreasonable burdens on insurance carriers.

Section 203. Notice of Confidentiality Practices

This section requires insurers to develop and provide notice of their confidentiality practices. The content of the notice is prescribed generally. In addition, the Secretary is required to develop model notices of confidentiality practices which, if used, would serve as a defense to an allegation that a violation of this section has occurred. We welcome the concept of the Secretary's model notice "safe harbor," and believe it could provide additional needed protection to insurers.

TITLE III—ENFORCEMENT

Section 301. Criminal Penalties

As outlined previously, the HIAA supports fair penalties for improper use and disclosure of health information. In this regard, we strongly urge you not to criminalize conduct that amounts to a mere technical violation of this proposed Act. The "knowingly" standard used in this section is not a sufficient bar to prosecution for such minor violations. If Congress believes criminal enforcement is necessary, we would strongly recommend that criminal penalties be an available remedy only where there is a knowing and willful material violation of the law.

Further, subsection (b)(3) would impose substantially heightened penalties for offenses committed with the intent to sell, transfer, or use health information for "commercial advantage." The draft legislation provides no definition of "commercial advantage." Broadly interpreted, these penalties would appear to conflict with many of the uses specifically recognized as valid under section 101 of the Act. For example, the payment policies of insurance carriers certainly are commercial in nature. To the extent health plans compete on quality and outcomes, quality assurance activities and accreditation processes also may be considered commercial.

These types of commercial activities are not only justified, but they are necessary to deliver quality health care to consumers. Furthermore, we believe it would be nearly impossible to craft a definition of "commercial advantage" that would not interfere with these kinds of beneficial commercial activities. Therefore, we urge you not to provide

criminal (or civil) penalties under the proposed legislation for commercial uses of health information.

Section 302. Civil Action

Subsection (a) of this section would grant a private right of action to any individual whose rights under the Act are violated. Because this private right of action as currently drafted extends to violations of all provisions of the Act-- including those that would amount to mere technical violations-- this section has the potential to exacerbate the recent trend toward the use of class action lawsuits against the health insurance industry and subject carriers to liability for significant damage awards. As noted previously, the HIAA believes that the impact of a private right of action may be partially minimized by adopting a materiality standard. The Draft NAIC Model Act, for example, extends a private right of action only to individuals who have been aggrieved by "material" violations of the Act. Even with this modification, however, the HIAA would continue to have grave concerns about increasing the industry's exposure to potentially frivolous lawsuits.

If a private right of action is provided by this Act, HIAA would support the two-year statute of limitations contained in subsection (c) of this section. We would also support the limitation in subsection (d), which would absolve insurers that disclose information consistent with the provisions of this Act from liability for such disclosure under common law. This is consistent with Section 20E of the Current NAIC Model Act.

TITLE IV—GENERAL PROVISIONS

Section 403. Relationship to Other Laws

As noted previously, HIAA supports national uniformity with regard to rules governing the use and disclosure of health information with limited exceptions for those rules reasonably needed to protect public health and safety. It appears that the general preemption language in section 403 of the draft legislation is intended to be relatively broad. It would preempt those state laws directly relating to matters covered by the Act. We would, for example, interpret this language to preempt all state laws requiring individual authorizations for use and disclosure of certain types of health information. Nonetheless, the preemption language in section 403(a)(1) is somewhat vague. We would recommend that additional language be added specifically preempting states from enacting or continuing in effect laws that duplicate, conflict with, or provide additional requirements with respect to the confidentiality of health information.

In addition, we have significant concerns about the exceptions to preemption in subsection 403(c)(3) of Representative Shays' draft legislation. This subsection would allow a broad exception to preemption for all state laws regulating information about an individual's mental health or communicable disease status. This exception would appear to save laws that go well beyond those designed to protect public health and safety through required reporting. In fact, this language could be interpreted to confer special status on state laws relating to use of these particular types of health information by health insurers and others.

In addition, we note that section 403(c) of Representative Shays' draft legislation would allow for the adoption of state reporting requirements which would be extremely difficult for insurers to administer and which could subject them to unwarranted liability. The May 1, 1998 Draft NAIC Model Act would require carriers to withhold disclosure of protected health information in instances in which: (1) the safety of a person may be jeopardized; (2) the information concerns sensitive health services; or (3) a minor who may lawfully agree to health care without the consent of a parent or legal guardian so requests. If enacted, these provisions would be extremely difficult to administer. These requirements could subject insurance carriers to private actions by individuals who do not want their protected health information to be disclosed to a policyholder, or by policyholders who assert a contractual right to know how the benefits under the policy are being utilized. Our companies are extremely concerned about the potential liability associated with suppressing disclosure of an explanation of benefits form to a policyholder, as well as with the operational feasibility of complying with such a requirement.

Section 405. Effective Date

The provisions of this proposed legislation reach to the heart of insurance transactional processes, and thus will have a major impact on insurers' core business functions from both administrative and systems perspectives. At present, most carriers are revising their computer systems to become "Year 2000" compliant, and are dedicating significant staff programming resources to accomplish this enormous task. Thus, even though the draft legislation provides for an 18-month delayed effective date, it is important to keep these

so-called "Y2K" efforts in mind as any confidentiality legislation moves closer to enactment.

In addition, we would recommend that Congress specifically provide for a negotiated rulemaking process with regard to any regulations developed under this Act, as it has with other matters of this complexity and magnitude.

Section 406. Definitions

The scope of definitions adopted in confidentiality legislation are extremely important to the feasibility of the overall Act

Specifically, the HIAA believes that the definition of "individually identifiable health information" in subsection (8) is problematic in part because demographic information is specifically included. At this point, the Draft NAIC Model Act does not extend the scope of individually identifiable health information to include demographic information. Insurers generally believe that restricting the use and exchange of demographic information, especially among affiliates, would unnecessarily limit their ability to communicate with policyholders about other available insurance options.

CONCLUSION

Once again, I appreciate the opportunity to testify before you today on this important issue. We look forward to working with you as you consider federal legislation to protect patient confidentiality. And we urge you to balance carefully the desire to assure confidentiality with the need for the private health care system to continue providing high-quality care to American consumers.

Mr. HORN. Well, thank you very much, Mr. Kahn. That's a very helpful statement.

Dr. Elizabeth Andrews is our last speaker on this panel. She's the director of Worldwide Epidemiology of Glaxo Wellcome, Inc., and appears on behalf of the Pharmaceutical Research and Manufacturers of America. Dr. Andrews.

Dr. ANDREWS. Mr. Chairman, and members of the subcommittee, as he said, I'm Elizabeth Andrews, director of Worldwide Epidemiology at Glaxo Wellcome, a leading research-based pharmaceutical company.

I really appreciate the opportunity to testify this morning on behalf of the Pharmaceutical Research and Manufacturers of America on confidentiality of patient medical information. We have submitted a statement for the record, so I will limit my remarks to a few key points.

PhRMA members discover and develop the majority of new medicines used in the United States and around the world. This year alone, PhRMA-members will invest more than $20 billion in research and development. Last year the industry brought 49 new prescription drugs and biologics to market, including new medicines to treat diabetes, cancer, heart disease, Parkinson's disease, HIV–AIDS, asthma, and other deadly and debilitating diseases.

Only with access to medical information that enables us to discover new medicines can a pharmaceutical and biotechnology industry continue this remarkable progress and help patients with unmet medical needs.

Revolutionary new diagnostic tests and treatments promise to expand and enrich our lives and the lives of future generations. Realizing this promise depends first, on research. It increases our understanding of human biology and the nature of disease. Second, on our creative ability to turn new knowledge into products that help people. Finally, it depends on epidemiologic help outcomes and pharmacoeconomic studies that inform us about disease, evaluate medical treatments, and measure the cost-effectiveness of therapies.

I'd like to summarize PhRMA's principles for maintaining the confidentiality of medical information, which are described fully in my written statement.

First, informed consent is necessary to protect the rights and welfare of individuals who participate in clinical trials. Second, researchers must have free access to data bases of medical information that does not directly identify patients. Third, existing laws and regulations effectively protect individuals who participate in federally regulated biomedical research, and new confidentiality legislation is not needed in this area. Fourth, all medical information that directly identifies individuals must be subject to uniform high standards. Last, national requirements should govern the use of medical information and research.

I would like to turn now to the legislation being developed by Representative Shays. We have had the opportunity to review the May 14 version which addresses many of the industry's concerns. Representative Shays appears to establish a workable framework for Federal legislation to protect the confidentiality of medical information. The drafters have recognized that a Federal system can

be established to protect a central public interest served by legitimate research uses of patient data, while protecting individuals' confidentiality interests.

As an epidemiologist, I'm pleased that the Shays' draft recognizes the importance of research using medical data archives, and acknowledges that patient confidentiality can be safeguarded without establishing insurmountable administrative burdens that would affectedly, make it impossible to use these archives.

PhRMA is also pleased that the bill recognizes the importance of the common rule and responsibility of institutional review boards. PhRMA supports strong penalties which the draft legislation contains, because we believe that penalties will help ensure that the confidentiality of patient is protected. And we support the bill's provisions for uniform national standards.

We did not read the Shays draft bill to require special authorization for research access to, and use of, medical information. Doing so, will treat research less favorably than other uses, and it could skew the data available to researchers and, if so, could impede research and adversely affect the public's health. There are a few technical corrections to the legislation of which PhRMA will work with Representative Shays, but we believe that the bill is an important step in confidentiality legislation.

Per the subcommittee's request, we have provided comments on S. 1921, Health Care PIN Act, introduced by Senators Jeffords and Dodd in our written testimony. I'd be pleased to respond to any specific questions you have on this bill.

Mr. Chairman, members of the subcommittee, PhRMA appreciates your efforts with respect to this important issue and your obvious attention to protecting the public's interest, while preserving the benefits of health research. We look forward to working with you as you continue your efforts whether in developing the discussion draft, or amending and perfecting legislation advanced by others. I'd be happy to answer any questions.

[The prepared statement of Dr. Andrews follows:]

Statement PhRMA

TESTIMONY OF ELIZABETH B. ANDREWS, Ph.D.
ON BEHALF OF THE
PHARMACEUTICAL RESEARCH AND MANUFACTURERS OF AMERICA
BEFORE THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY OF THE GOVERNMENT REFORM AND OVERSIGHT COMMITTEE

May 19, 1998

Introduction

Mr. Chairman and Members of the Subcommittee, my name is Elizabeth Andrews, and I am Director of World Wide Epidemiology for Glaxo Wellcome, a leading research-based pharmaceutical company. I would like to begin by thanking you for the opportunity to testify this morning on behalf of PhRMA, the Pharmaceutical Research and Manufacturers of America, on the important issue of federal legislation to protect the confidentiality of medical information. PhRMA represents the nation's leading research-based pharmaceutical and biotechnology companies, which discover and develop the majority of new medicines used in the United States and around the world. PhRMA's member companies will invest more than $20 billion this year alone on research and development. Last year, the industry brought 49 new prescription drugs and biologics to market, including new medicines to treat diabetes, cancer, heart disease, Parkinson's disease, HIV/AIDS, asthma, and other deadly and debilitating diseases.

Medical Information is Essential for Research

We are pleased that this Subcommittee will play a leading role in crafting patient confidentiality legislation, and we look forward to working with you. As an association of the nation's leading research-based pharmaceutical and biotechnology companies, PhRMA recognizes that we all must trust that the confidentiality of medical information that identifies us will be protected. By understanding our responsibility and upholding this trust, pharmaceutical companies can continue to discover and develop new medicines that make people's lives better. Research on new medicines depends upon patients' willing participation in medical research and researchers' access to reliable medical information.

The pharmaceutical and biotechnology industry can help patients with unmet medical needs only if researchers have access to medical information that enables them to discover new medicines. Today, medical researchers are poised to make countless new discoveries. Revolutionary new diagnostic tests and treatments promise to extend and enrich our lives and the lives of future generations. Realizing this promise depends on research: basic research that increases our understanding of human biology and the nature of disease and disability, and applied research that enables us to turn new

knowledge into products that help people. It also includes epidemiological, health outcomes, and pharmacoeconomic studies that inform us about disease, evaluate medical treatments, and measure the cost effectiveness of therapies.

PhRMA Principles for Patient Confidentiality

To both reassure patients that medical information will kept confidential and to ensure that researchers have access to reliable medical information, PhRMA developed the following principles for maintaining the confidentiality of medical information that directly identifies individuals, which it offers for the Subcommittee's consideration:

1. When individuals participate in clinical trials, informed consent is required to protect their rights and welfare. Clinical trials to study the safety and efficacy of new medicines cannot be conducted without the voluntary participation of individuals.

2. Researchers must have free access to databases of medical information that does not directly identify patients. Some of the most important medical research does not require interaction with a patient or provider, but instead relies on archival medical data. These archives are a valuable public health resource. Legal, technical, and practical mechanisms – including encryption, contractual and statutory limitations on permissible uses and users, and strong penalties for using the data to identify an individual – can effectively protect individuals whose medical data are archived. PhRMA supports legislation that implements such protections while preserving the research use of these data.

3. Existing laws and regulations effectively protect individuals who participate in federally regulated biomedical research; new confidentiality legislation is not needed in this area. In 1991, sixteen federal agencies, including the Food and Drug Administration, adopted the "Common Rule" to protect people participating in research from undue risk. The Common Rule protects individuals through oversight by Institutional Review Boards (IRBs), which review the risks posed by research and the protections in place to safeguard participants' well-being, including preserving the confidentiality of medical information identifying them.

4. All medical information that directly identifies individuals must be subject to the same high standards. PhRMA member companies cannot support any separate, implicitly "higher" standard of protection for genetic, psychiatric, or infectious disease information. Instead, legislation should protect the confidentiality of all patients, whatever their condition.

5. Uniform national requirements should govern the use of medical information in research. Without federal preemption, states can establish and enforce a multiplicity of contradictory requirements and standards. A patchwork of inconsistent state laws and regulations would erect impassable barriers to conducting important medical research. Clinical trials and epidemiologic studies cross state borders. For an issue as important as the confidentiality of medical information, there is no alternative to

federal legislation that establishes the same high standards of protection and rights for individuals, no matter where they reside, work, travel or fall ill.

S. 1921, the "Health Care PIN Act"

Having outlined PhRMA's principles, I would like to highlight our concerns with S. 1921, the "Health Care PIN Act," sponsored by Senators Jeffords and Dodd. First, the bill's core definitions fail to provide a workable basis for strong confidentiality protections.

- Researchers are permitted to use "nonidentifiable health information," but this term is defined so narrowly that no useful epidemiologic or outcomes research could be undertaken.

- "Protected health information" is defined too broadly, making it necessary to obtain specific informed consent for each use of a database containing information that only indirectly identifies individuals.

- Encryption methodologies (or "anonymous links," as the bill refers to them) could be effective security mechanisms. In S. 1921, however, they are only used to establish penalties for the use of a database that theoretically could be linked to individual identifiers – even if the researcher does not identify individuals. The language n the bill could be improved to assure that the linkage key itself is properly safeguarded and that databases code information and do not directly identify individuals can still be available to researchers.

Second, S. 1921 would impose additional requirements beyond those that guide FDA's oversight over postmarketing surveillance of a drug's safety and efficacy. It would transform the Common Rule governing biomedical research in ways that are inconsistent with PhRMA's principles and, more importantly, could hinder vital research. The bill also gives the Secretary of Health and Human Services new authority to regulate all research activities. Such sweeping changes in public policy and the regulation of research deserve separate, thoughtful deliberation, and should await the report and any recommendations of the National Bioethics Advisory Committee (NBAC) and the National Institutes of Health (NIH), which are reviewing existing Common Rule requirements. Broad changes to research policy and regulation should not be an afterthought in confidentiality legislation, where they must compete for attention with many complex issues.

Finally, by including broadly drafted exceptions, S. 1921's preemption clause does not achieve its purpose. As a result, research, health care, and patients' privacy rights will continue to be governed by a patchwork of different laws for different types of information in different states.

Draft House Legislation

We have had only a brief opportunity to review an early version of a draft bill being circulated by your staff, Mr. Chairman. We have received a more recent version of the draft bill, and would be pleased to provide you our comments shortly. A preliminary reading of the earlier draft suggests that the drafters may be trying to accommodate several significant research concerns. For example, the draft would exempt research conducted under an "investigational new drug application" from new confidentiality requirements, which would permit clinical trials to continue to be governed by the Common Rule. It is unclear, however, why other research governed by the Common Rule, such as studies on pediatric indications for a drug already approved for use in adults, should not be similarly exempted from new or additional regulatory requirements.

The draft bill also attempts to ensure the availability of databases of "anonymized" information and to protect postmarketing surveillance of safety and efficacy. Likewise, the draft bill's treatment of preemption suggests an intent to find a workable basis for uniform federal standards. With respect to these important issues, the drafters' intent seems consistent with PhRMA's principles and we welcome the opportunity to work with you to draft the best possible language.

In other areas, however, the draft bill causes concern. For example, among the prohibited acts included in the bill is "negligent or intentional disclosure . . . by a person granted authority under an authorization . . . ," but does not establish a framework specifying when, how, and by whom health information *should* be used. As a result, it is unclear why or whether anyone would obtain an authorization.

Epidemiological Uses of Data

You have asked me to speak specifically to the use of medical information in epidemiology. As an epidemiologist, I have been particularly involved in the study of HIV/AIDS and sexually transmitted diseases, the medicines developed for such conditions, and the risk of medicines when used in pregnancy. In these areas, we have made significant strides, coupling drug development programs with company-sponsored public health monitoring activities. Through such efforts, we ensure the safe use of products developed to treat many serious diseases.

Many examples of important observational research are available. I would like to call your attention to two discoveries that would not have been possible without access to archived medical information.

- An epidemiological study in the early 1980s that found a strong association between the potentially fatal Reye's syndrome and children's use of aspirin.[1] Eventually, this

[1] T.J. Halpin et al., "Reye's Syndrome and Medication Use," *Journal of the American Medical Association*, 13 Aug 1982: 687.

new knowledge led to a decline in cases of Reye's syndrome in the United States, improving children's health and reducing mortality.

- A recent study documented both the under-use of beta-blockers following myocardial infarction in the elderly, and the serious consequences of that under-use.[2] This study linked large pharmacy and medical claims databases. Its finding of unnecessary deaths and hospitalizations from cardiovascular episodes is likely to lead to basic changes in medical practice and greatly improve patient health.

- In the critical area of HIV, in which approval of new therapies occurs at a fast pace, much of what we learn about drug safety and effectiveness is learned through the use of observational data after drug approval. For example, we learned from observational experience that differences in HIV disease progression seen by gender, race and intravenous drug use were not due to those patient characteristics, but due to differences in treatment and access to treatment.[3,4] Observational studies demonstrated the effectiveness of pneumocystis carinii pneumonia (PCP) prophylaxis,[5] and quantified the adverse experience rates with antiretroviral therapies and various treatments for opportunistic infections.[6] All of these findings have contributed to more effective care and better outcomes for patients with HIV

In addition to the public health value of these large-scale studies, health care payers in our cost-conscious system demand more focused outcomes research and economic analysis to select the most efficacious and cost-effective treatment options. For example, Harvard Medical School researchers found that restrictions on the use of schizophrenia medications in the New Hampshire Medicaid program proved penny-wise but pound-foolish.[7] The restrictions yielded some savings on prescription drugs, but ultimately increased state and federal government Medicaid spending overall by sharply increasing the need for emergency care and hospitalization. The Harvard team produced these findings – which can promote both better health care for patients and more cost-effective use of health care dollars – by linking prescription drug use databases with mental health center and hospital data.

---

[2] N.F. Col et al., "The Impact of Clinical Trials on the Use of Medications for Acute Myocardial Infarction. Results of a Community-Based Study," *Archives of Internal Medicine*, 8 Jan. 1996: 54.

[3] R.D. Moore, D. Stanton, R. Gopalan, et. al., "Racial Differences in Drug Therapy for HIV Disease in an Urban Community," *New England Journal of Medicine 1994;330:763-8.*

[4] R.E. Chaisson, J.C. Keruly, and R.D. Moore, "Race, Sex, Drug Use and Progression HIV Disease," *New England Journal of Medicine* 1995;333:751-6.

[5] R.D. Moore and R.E. Chaisson, "Natural History of Opportunistic Disease in an HIV-Infected Urban Clinical Cohort," *Annals of Internal Medicine* 1996;124:633-42.

[6] R.D. Moore, I.S. Fortgang, and J.C. Keruly, et. al., "Adverse Events from Drug Therapy in HIV Disease," *American Journal of Medicine 1996;101:34-40.*

[7] Stephen B. Soumerai et al., "Effects of Limiting Medicaid Drug-Reimbursement Benefits on the Use of Psychotropic Agents and Acute Mental Health Services by Patients with Schizophrenia," *New England Journal of Medicine*, 8 Sept. 1994: 650.

Conclusion

Mr. Chairman, Members of the Subcommittee, I again wish to express PhRMA's appreciation for your efforts with respect to this important issue and your obvious attention to protecting the public's interest in the fruits of health research. We look forward to working with you as you continue your efforts, whether in developing the discussion draft or in amending and perfecting legislation advanced by others.

APPENDIX

Dr. Elizabeth B. Andrews, M.P.H., Ph.D., is Director of Worldwide Epidemiology at Glaxo Wellcome, based in Research Triangle Park, North Carolina and Greenford, England. The epidemiology program encompasses epidemiologic drug safety studies, natural history of disease studies, disease burden studies and descriptive epidemiology. The program has included a series of safety studies of oral acyclovir, zidovudine, azathioprine, and the natural history of epilepsy, advanced rheumatoid arthritis, cerebral toxoplasmosis, and HIV disease progression. A recently completed study evaluated the ability of patients to recognize sexually transmitted disease (STD) symptoms and to seek appropriately diagnosis and treatment. Her work of the impact of antenatal steroids and neonatal mortality and morbidity, conducted with information in company surfactant databases, was presented in the NIH-sponsored Consensus Development Conference on the Use of Antenatal Steroids for Fetal Maturation.

Dr. Andrews' department manages prospective pregnancy registries for acyclovir, valacyclovir, antiretrovirals, sumatriptan and lamotrigine to monitor for the risks of drug-related teratogenicity. Treatment INDs have assessed safety, survival, and other endpoints associated with treatments for HIV in adults and children, pneumocystis carinii pneumonia (PCP), neonatal respiratory distress syndrome, and non-small-cell lung cancer. The department makes extensive research use of large population-based databases, including public access files of the U.S. National Center for Health Statistics, to estimate unmet medical needs in the long-range planning activities of the company.

Dr. Andrews serves as an Adjunct Assistant Professor of Epidemiology at the UNC School of Public Health. She is a member of the Pharmaceutical Research and Manufacturers of America (PhRMA) Clinical Safety Surveillance Committee and chairs its Epidemiology Subcommittee. She is a member of the editorial board of the journal Pharmacoepidemiology and Drug Safety. She is a member of the International Society for Pharmacoepidemiology, serves on its Board of Directors, and currently chairs its *Ad Hoc* Committee on Data Privacy in the U.S. and Canada, and serves on its Public Policy and Ethics Committee.

Dr. Andrews received her MPH in Health Policy and Administration and Ph.D. in Epidemiology from the University of North Carolina School of Public Health. Prior to joining Burroughs Wellcome in 1982, she managed the Statewide Regionalized Perinatal Care Program and directed the Purchase-of-Care Services for the State Health Department of North Carolina.

Dr. Andrews is testifying on behalf of the Pharmaceutical Research and Manufacturers of America (PhRMA). PhRMA is aware of the new House rule, adopted January 7, 1997, requiring certain disclosures by public witnesses. PhRMA has not been awarded any government contracts or grants during the current fiscal year or two previous years.

The testimony presented today is on behalf of the association, not any individual member company or group of member companies. PhRMA makes no representation with regard to any federal grants or contracts, if any, received by any PhRMA member company.

Mr. HORN. We thank you very much, and we're going to be pursuing some of the issues that you've mentioned.

What I'm going to do is yield myself 10 minutes to start the questioning, and then I'll yield to Mrs. Maloney, the key representative on this committee from New York, and a former ranking member. She will have 10 minutes and then we're going to get to a dialog. What I want to do in very succinct terms on your part, is pose a couple of questions and I'd just as soon you answer them in not more than 30 seconds. I don't want a filibuster, I just want to get the best thinking you can give us on that spur of the moment. I find wisdom often comes that way, as opposed to sometimes bureaucratic statements. Not that yours are bureaucratic. They're very thorough, but sometimes they appear that way.

So, I guess I'd start with you Dr. Andrews, and just move right down the line. What do you think the problem is that we're trying to solve with this legislation and where should our focus be?

Dr. ANDREWS. One of the problems is a public perception and fear that there are not adequate safeguards covering the use of——

Mr. HORN. I'd like to get the microphone closer to you please.

Dr. ANDREWS. Sorry. I think that one of the main problems is that the public perception that their privacy is not adequately safeguarded. So I think it is important for us to review the safeguards that are already in place to reassure the public that many protections are available. I think it's important that we look at safeguards that strike the right balance between providing better assurance of confidentiality protections, while also assuring that we protect the public by gaining additional data through research on the safety, effectiveness, and cost-effectiveness of our medical interventions; that we protect the larger good, as well as, the individual concerns.

Mr. HORN. Mr. Kahn, do you agree with that statement or would you subtract something or add something?

Mr. KAHN. I would agree with it. I would add that, other than protecting the consumer, the key here is to prevent misuse, particularly, willful misuse of medical information or health information.

Mr. HORN. How about it, Dr. Harding, do you agree with the two preceding speakers on the definition? And where would you say they're wrong and where are they right?

Dr. HARDING. I would say that the American citizen is concerned about their privacy as it goes out from their individual knowledge to their physician and beyond, and that this mistrust in what is beyond that point has led to the great concern that we're all sitting here trying to address—laws of trust.

Mr. HORN. Ms. Frawley, do you agree with the preceding three speakers or have they missed something?

Ms. FRAWLEY. I agree with the three, and the only thing that I would add is the fact that I think that patients need to have some control over the use of their information. And I think that's something that we have lost in some degree. So, I think——

Mr. HORN. You need to speak closer into that microphone. They're terrible microphones.

Ms. FRAWLEY. I know. The concerns regarding redisclosure of information. If I said I want my information going here, I don't ex-

pect to find it going down the information chain to people that I didn't contemplate. So, the example, in terms of Giant and CVS, they ask for my prescription to be filled. I didn't ask for my information to be sent off somewhere else, so I think that is an important piece of any legislation.

Mr. HORN. Dr. Korn.

Dr. KORN. Well certainly, sir, I think I agree with the general thrust of those answers, even though the newspapers, the Post, the Times, and probably others have had long feature stories in recent months about how easy it is to get any information one wishes about just about anybody, if one knows where to go and has a few hundred bucks to spend. I think the trick, sir, is to try to keep the protections on the perimeter of the health care delivery and research systems and build those protections so that the information that patients and physicians share is secured to the maximum possible extent within that perimeter, rather than trying to drop barriers inside the perimeter and disrupt the flow of information that, I think, most of us believe is essential to allow the health care delivery system to function, complex as we've created it, but that's what we have, and to promote the continuation of medical research.

Mr. HORN. Mr. Nielsen.

Mr. NIELSEN. I agree with most of what's been said. In fact, all of it, really.

Mr. HORN. Do you disagree with any of it?

Mr. NIELSEN. I can't say it as eloquently as Dr. Korn has just said it, but I think we can do wonderful things in medicine these days using technology and using the electronic transfer of patient information. I mean, we save hundreds and hundreds of lives, and we ought not to be enacting legislation that impedes our ability to do that. We've somehow got to balance the understanding of the protection of privacy with these kinds of things that we can do.

These bills sometimes use the words "ensure privacy." I don't know that in the context of what we're talking about, we can ever ensure it completely. What we can do, though, is to protect it as well as we can, and punish those who abuse it.

Mr. HORN. Ms. Goldman.

Ms. GOLDMAN. Mr. Chairman, I believe that it's the absence of a national health privacy law that impedes access to complete and accurate data for research on public health initiatives. People can no longer trust, and with good reason, that the information that they share within the four walls of their doctor's office will remain there, and that it will be used for purposes related to their care, related to their treatment, and related to the payment of their claims. They have no idea, because they're not asked for their permission, and they're not given notice about other uses.

Some of those uses are laudable and will advance public health initiatives. Some of them might not be as laudable. People should be able to make those choices at the front end, and they can't now, and I think it's leading them to withhold information, giving accurate information, and maybe not seek care at all. So the truth is, I think that it's the absence of the law that's really standing in the way of advancing, to the fullest extent we can, some of these critical public health initiatives that we've heard about.

Mr. HORN. Let me ask you, Ms. Goldman, we'll start down line on the patient authorization and informed consent. Is that needed n every occasion or are there exceptions that should be made to hose occasions where there is consent given by the actual person vhose medical records are involved?

Ms. GOLDMAN. As a starting point, the foundation of any Federal privacy law, whether it's protecting video rentals, credit records, or inancial records, is providing for the ability for people to give con- ent prior to disclosure. That's the general principle that we start vith.

Clearly, there has to be exceptions to that. No right is absolute, ncluding the right to privacy. So, where there's an emergency, for nstance, you can't get consent; where there's a public health man- late or disclosure of information to the public health department; vhere law enforcement has presented a warrant or some other egal process, or where there is a fraud investigation going on. Those are not situations where I think we can require consent be- ause then it would so interfere with those other activities.

But I think we need to start, as a general rule, with giving peo- ple information about how the data will be used and allowing them o make choices. People can make these choices in an informed and educated way, and I think that it will strengthen the health care environment.

Mr. HORN. Mr. Nielsen.

Mr. NIELSEN. I agree with that. I'd go even a little bit further o suggest that authorizations or consent are expected in this par- icular arena. And for that reason, I think, we would prefer the construction of the Bennett-Jeffords versions which require patient consent.

Mr. HORN. Dr. Korn.

Dr. KORN. Yes sir, I try to deal a little bit with the consent issue n my remarks, and there's much more in the written statement hat we've submitted for the record.

I think consent is a tricky issue, as I said, when it comes to ac- ess to historic materials. It's tricky because, in fact, you cannot in any full and informed way describe what may be a very important, exciting opportunity on a particular kind of disease that would ben- efit from going back and looking at historic experience, whether hat's a record or a blood sample, or a tissue sample, or whatever else. It's logistically impossible to do a consent every time you want access to these materials for a lot of reasons. But two of them are hat often these materials are quite old, and one doesn't know vhere the individual may be; they may have moved; they may have passed away. Another reason is that these materials are brought ogether and examined in very, very large numbers in order to get he samples that one needs to do the particular kinds of studies, and that may be hundreds or thousands or tens of thousands of samples.

And, if you just think about trying to go back over a period of years to very large numbers of individuals to try to get reconsent, which is another term that's used in this discussion, that's just not feasible. I mean, it just simply won't work and the work won't be done because it will be too burdensome. In fact, I think it would be largely impossible.

So, we believe, that for retrospective studies of materials, even if they have identifiers on them, that is, patient identifications, which we don't think is commonly needed, but may be needed in some instances, that having a process of review of the research proposal, either the IRB or an equivalent body in non-common-rule organizations that is able to weigh the importance of the study and decide whether, in fact, the investigator needs identified information, is the only logical way to go on this.

Mr. HORN. In response to that, since I want to finish this question, Ms. Frawley, do you agree or disagree or what's been left out so far?

Ms. FRAWLEY. I certainly agree with the remarks. I will followup in terms of Dr. Korn's statement. I think it's important that we keep in mind that there are times when we have to go back and call back patients into the system.

And two personal experiences I was involved in was trying to locate women who had taken DES, and trying to get them back into the care system, and also, individuals who had received blood transfusions that possibly need to be tested for HIV. Those are very complicated issues because again, the records may not be current in terms of patient location. So, the concept of trying to go back to patients to get consent for research purposes or to bring patience back into the system are sometimes problematic.

But, we would support the approach that both Senator Bennett and Senator Jeffords have taken in terms of authorization.

Mr. HORN. OK. Dr. Harding, any comments?

Dr. HARDING. The only additional one, would be the emphasis on noncoercive consent; that your consent not be related to health information or health insurance or job, the issue of employer-employee relationships that changes consent to coerced consent.

Mr. HORN. OK. Mr. Kahn, anything to add or subtract?

Mr. KAHN. I guess all I would add is that consent is key to maintaining confidentiality, but there has to be some, when the rules are actually drafted, there has to be some reasonableness, because when you get into issues of fraud and abuse in trying to use information to prevent information to prevent fraud and abuse, if the rules are too tight, you won't be able to use the information.

Mr. HORN. Dr. Andrews.

Dr. ANDREWS. I'd like to make just two points. One, is that I agree with Dr. Korn's earlier statement that it would just cover it adequately, I believe, in the Shays draft that for information that has been rendered anonymous or data bases without identifiers I don't believe consent is necessary.

But, I'd like to highlight the drug surveillance activities that are performed by the pharmaceutical companies and the Food and Drug Administration. If a physician is reporting to a company about a patient who has had a serious, life-threatening, adverse experience to a medication they've been taking, it would not serve the public well for the patient to refuse to give consent for that information to be shared. If we did not have the ability to capture that information without patient consent, then that loss of information may deprive us of important safety information on medical products that the companies and the Food and Drug Administration

will use to prepare additional information that will allow the medication to be used more safely for patients in the future.

Mr. HORN. Thank you.

I now yield 12 minutes to Mrs. Maloney, since I ran over too.

Mrs. MALONEY of New York. OK, thank you. This is an incredibly important issue, and I thank the chairman for calling this hearing on this really important area.

I would just like to ask each of you very briefly, as all of you know, Congress was given a 3-year window to come up with health care privacy legislation. And if no legislation is passed, the Secretary is required, by law, to issue regulations. Can I, just briefly, starting with Ms. Goldman, just go down and answer whether you prefer Congress or the Secretary to come forward with the solution? Just say, "Secretary" or "Congress."

Ms. GOLDMAN. Congress. [Laughter.]

Mrs. MALONEY of New York. Congress.

Ms. GOLDMAN. I mean, I think it's very basic here that we have an opportunity, in this body, to enact legislation which is specific, which is tailored. The Secretary will still have an opportunity to issue regulations to flesh out particular provisions, but this is where we can get an enforceable law with penalties in place and really have a more deliberative process.

Mr. NIELSEN. Agree, completely. Many of us on this panel have been working diligently for over 2½ years on this issue, and I think we're close to a congressional solution. We much prefer that.

Dr. KORN. Yes, ma'am. I agree with them.

Ms. FRAWLEY. Same answer.

Dr. HARDING. Congress.

Mr. KAHN. When HIPAA was drafted, the 1999 date was a backstop, and clearly the intent of Congress was to provide Congress time to act and we think Congress should take action in this area.

Dr. ANDREWS. We think that the rules and the content are more important than who proposes or adopts them.

Mrs. MALONEY of New York. OK. As you know, this has been a hotly debated issue. We have not been able to come forward with any type of consensus. Can you tell me what you see as the major roadblocks to passing some legislation? There have been many, many attempts in the past. We haven't succeeded. What do you see as the roadblocks? Why can't we pass it? Just go down the line again, very briefly.

Ms. GOLDMAN. I don't want to make too much at this stage of roadblocks because I think that we haven't yet really started the deliberative process that we need to—we, at this table and others who are concerned about this issue—to address issues one at a time, and really see where we can read some common ground. I think that process will begin. I think it's starting, but I think that we will be able to reach common ground.

Preemption, again, is a tough issue, and it's one I would suggest we reserve until the end of the day, until we see where we've been able to reach agreement on other issues. I think the actual details embodied in the authorization language also have provided us with some disagreements.

I would say in the research area, I actually find a tremendous amount of agreement in terms of looking at the Federal regulations that currently exist, making sure that they continue to apply and applying them to the private sector. I'm seeing more and more agreement in that area. So, I think that, particularly, in looking at some of the details is where we really have to sit down and start the process of reaching common ground.

Mr. NIELSEN. I can tell you, with assurance, that we are a lot closer to agreement on consensus than we were 2 years ago when Congress was considering this. And I think at that time it was viewed as such a divisive issue that no one really wanted to tackle it. We are getting very close, I think.

Mrs. MALONEY of New York. What's your favorite bill? We'll add that to the question. [Laughter.]

We've got quite an assortment.

Mr. NIELSEN. Well, that's fairly easy and I must be a little too hopeful——

Mrs. MALONEY of New York. What's your favorite bill? Just tell me.

Mr. NIELSEN. I'm from Utah, so Senator Bennett's bill is my favorite bill. [Laughter.]

Mrs. MALONEY of New York. OK.

Dr. KORN. I think the answer to your question is that I don't think most people realize the extent to which medical information does flow and has to flow in order to keep our health care delivery system functioning and to permit medical research to take place. I think, Ms. Goldman, in one of her comments earlier, developed the image of the patient and the physician within four walls.

Well, we don't live in a society or in a health care system that's like that anymore. We want someone else to pay for our care. For example, take medical transactions in cash: You might be able to have more privacy if you insisted on it, just like you could if you bought everything with cash and didn't use plastic credit cards. So, I think that part of the problem in this debate is the very lack of awareness of the ordinary citizen on how our health care system actually works.

I think a second issue, and it's one that I just want to reemphasize, is that we feel strongly that because of the way care and research are done, that a strong Federal preemption is very important. We understand the issue that certain kinds of diseases are considered to be sensitive, but I would argue that to a victim of a disease, every disease is sensitive.

I had the privilege of chairing the National Cancer Advisory Board for 7 years and heard heart-rendering stories from people who had been diagnosed with cancer and were afraid of losing their health insurance, losing their job, being stigmatized. So, there isn't just one disease that people can use hurtfully against other people. Many diseases or most diseases can be used that way. I think that once one starts carving out categories of disease from preemptive language, one is on a very, very, "slippery slope."

Mrs. MALONEY of New York. What's your favorite bill?

Dr. KORN. Well, I tell you, frankly, ma'am, I can't keep them all straight. They come in such profusion. But at the moment, I think the Shays bill is very, very thoughtful and I think that the latest

version that I received yesterday evening of the Bennett bill is a very, very, positive bill. I think that bill shows an incredible amount of maturation over the last couple of years.

Ms. FRAWLEY. A major concern is certainly, as Dr. Korn pointed out, is the whole preemption issue. If we allow information to be carved out or segregated, we're going to have a problem because any time we have a request for information we will have to say to the requester, "I'm sorry, I need a different type of authorization," or "I need a court order and served as a subpoena." So, I'm really concerned about any bill that would carve out exceptions for sensitive information. As Dr. Korn pointed out, all information deserves the same high level of protection.

The other area of concern that I think we need to focus on is the amount of information that is needed. So, one of the things I will raise is the fact that routinely, our members are in a situation where information is sent forward to a third-party payer, and then a request comes back saying please forward us a complete copy of the medical record before the claim will be paid. And we have people standing at xerox machines all around the United States xeroxing records everyday, and sending them off.

I would argue that one of the things that legislation needs to talk about is: How much information do you legitimately need for particular purposes? And, when can information be used in nonidentifiable ways? I think there's a lot of identifiable information that is going out the door and, that possibly, that use could be fulfilled by the use of nonidentifiable information.

People are concerned that their employers have access to their health information. We have employers who are self-administering benefit plans, who are receiving health information, and are using that information to make promotional decisions in the workplace, and that's wrong.

Mrs. MALONEY of New York. What's your favorite bill?

Ms. FRAWLEY. I have the Chinese-menu approach, I did an analysis of the four bills and the two drafts that I can take you through each of them and tell you which piece I like.

Mrs. MALONEY of New York. That sounds like the Horn bill. [Laughter.]

Mr. HORN. Please file that for the record at this point.

Mrs. MALONEY of New York. OK. Yes, that would be helpful. OK.

Dr. HARDING. Well, I would talk on the other side of the sensitive information, partition of medical record issue. It seems to be very important.

I would like to think as a psychiatrist that all information would be handled so thoroughly and privately that we wouldn't have to have a differentiation between psychiatric, infectious disease, obgyn, and some of those issues that are very important to the individual even more than a twisted mean. So that if we can raise the bar to that level, I would certainly be in favor of not having a partition of the medical record. But, without that, I still feel that that would be a valuable commodity to have in any legislation.

On favorite bill, at this point would still be the Leahy-Kennedy bill.

Mrs. MALONEY of New York. OK, thank you. Mr. Kahn.

Mr. KAHN. Yes. I would argue that if the Congress searches for the perfect legislation to dictate the process for protecting or preserving privacy, that it will fail. Instead, it seems to me that, there is no perfection here, and that instead, the objective ought to be a deterrent to misuse or abuse of information. And I think that needs to be the key objective and key ingredient.

Second, obviously, uniformity is important. Any kind of State-by-State rule-setting in this area will lead to chaos, particularly, in the electronic age.

And we would prefer the Shays bill.

Mrs. MALONEY of New York. The Shays bill, OK. And Dr. Andrews.

Dr. ANDREWS. Yes, roadblocks are barriers to effective legislation. I think it's because of the complexity of these issues. The complexity really defies very easy solutions. And lack of understanding about how medical information must flow freely within the health care system, and how research makes use of health care information to ultimately protect patients and population.

I think that, for example, we don't have as good an understanding in the public about the fact that research doesn't recognize geographic boundaries. And the promulgation of individual laws in individual States may not serve any additional protection for individuals, but may serve to impede the progress of research and provision of medical care.

We need to focus more on the establishment of penalties for misuses of information and adequate safeguards to govern the appropriate use of information.

We feel that in terms of favorite bills, that Shays is headed in the right direction. And, although, I haven't seen the most-recent version of the Bennett bill, it was also heading in the right direction.

Mrs. MALONEY of New York. I would like all of you to hand-in to the chairman's committee what you must have in the bill and what you would most like to have out of the bill from all of these drafts.

I want to go back to the issue that he raised on really the source of identifiable information, which is somewhat critical. I have heard stories that some doctors will sell lists of their patients that are certain drugs or treatments or whatever; that some pharmacists sell these lists. I don't know if it's true or not, but I've been told it, and I think that's a terrible violation of personal privacy.

It would be helpful to learn about how the private-sector deals with medical information. And there have been increasing numbers of press reports about companies receiving and using identifiable information, containing such information as names and Social Security numbers. I think, all of us would say that is a gross invasion of a person's privacy. If people are receiving—you know, in medical research you don't need the Social Security number, and you don't need the name. You may need the information, but you don't need that personal information.

So, I'd like to ask all of you the same question again, if I could. But let me start with Dr. Andrews. As a representative of a pharmaceutical researcher and manufacturer, can you tell me how your

company received or receives identifiable information? Is it received with the consent of the individual?

Dr. ANDREWS. First of all, we rarely receive identifiable information. Most of the information that is used in the search for clinical trials or for epidemiologic or health outcomes research is received within the company, if it is indeed analyzed within the company in a form that has taken the identifiers off of the information. There may be a code within the data base that can be used back with the treating physician or the investigator, who is actually not a company employee, but may be an employee of an academic research institution, for example. The researcher would have a master list of those codes that are contained in the research——

Mrs. MALONEY of New York. So, you don't need identifiable information?

Dr. ANDREWS. For research we do not need identifiable information. There are a couple of exceptions where we may have identifiers for a short period of time. One of those examples would be in the reporting of adverse experiences in which we may need to contact the reporting physician who calls the company to report an adverse experience to one of our products. We may maintain some code or identifier short of the name or address, but perhaps initials so that we could track back with that physician to gain additional information to help understand that adverse experience.

We also may, for a short period of time, have some identifiers in other safety studies. The example that I use is pregnancy registries. What you may or may not be aware of is when we develop medications during the clinical trials program, it is considered unethical to provide treatment of a pregnant woman for most clinical trials. The only way that we learned about the safety of medicines when given during pregnancy is through some observational approach. We've established within a number of companies, registries to evaluate drug safety in pregnancy does manage to some extent, like the reporting of adverse experience in which a physician will call the company usually asking for information about safety——

Mrs. MALONEY of New York. So when you do receive information that is identifiable, do you receive it with the consent of the individual?

Dr. ANDREWS. In most safety reporting examples, it is up to the physician and the patient to have a dialog about consent. We do not require consent in that case. We only maintain an identifier in that case, at the request of the physician. For example, if we're following a pregnancy, from the time of reporting which may be very early in pregnancy, and our intent is to determine the outcome of the pregnancy. Did the infant experience problems? Were they healthy at birth, or did they have a congenital abnormality? We need to be able to follow months into the future.

The average practicing physician is not in the same situation as a clinical researcher where they have the research infrastructure for keeping codes. They need to provide——

Mrs. MALONEY of New York. OK. My time is up. So, I'd like to ask a yes or no question, just run down the aisle. Is it necessary to have identifiable data? Yes or no?

Mr. KAHN. Yes, for claims purposes and paying for services that are provided for people it is necessary. But there is always permis-

sion asked, if a person wants a claim or service paid for by an insurer, then they have to give approval for that insurer to have access to the information regarding the service provider.

Mrs. MALONEY of New York. OK.

Dr. HARDING. Yes, for treatment and payment that we should ensure that deidentified data be used in every circumstance as possible.

Mrs. MALONEY of New York. But how do you do that?

Ms. FRAWLEY. You need to identify the information for treatment, payment, and health care operations, and then in other areas, one could probably use disidentified information.

Dr. KORN. As I mentioned in my oral testimony, I think the vast majority of research does not need the actual name of the research subject, but they do linkage which is the kind of thing Dr. Andrews was talking about. In other words, let me take just 1 second if I may.

If we're trying to study the effect of taxol in preventing recurrent breast cancer, you start with a population of people who have been diagnosed with breast cancer. You want the subgroup that has received taxol. All that can be done with codes. But then you want to know 5 years later, what happened to these women, and you have to be able to get records or experiences of each woman that map to the one you started with. The only way to do that is to have a code that is uniquely linkable to the individual. If you understand what I mean, the code cannot be anonymous in the sense that no identification possibility ever remains. That you cannot do. But you don't need a name. You could have a 25-digit code number if you want, or whatever it might be as long as there's linkability.

Mr. NIELSEN. Yes, for the reasons Ms. Frawley indicated. I'm sorry, Mr. Chairman.

Mr. HORN. Just let me ask, Dr. Korn, who keeps the identification of the real name and address? The doctor? The doctor might die, retire, go to Bali?

Dr. KORN. That's an extremely difficult question, Mr. Chairman. There are repositories of materials that have been created for research under NIH auspices where the originating provider, that is, let's say the originating hospital, will send material to a federally supported research collection with pertinent information that describes what the material is all about, with a code. So in that instance, the originating hospital will be the site of the keys.

Within a given large academic medical center, take Johns Hopkins or Stanford or Columbia or P&S or whatever, in order to do a true deidentification of all the data used in everyday research will require the creation of a system that will have to transpose these records and materials and put identifying codes on them that are not an individual's name, but if tracked, uniquely go back to an individual. And then, those keys, that is the linkage points where code and name are together, will have to be kept secure. It will have to be protected from trespassing. I don't think there's any other way to do that. It's going to be expensive.

Mr. HORN. Well, I want to make sure you answer Mrs. Maloney's question, the last two of you. So why don't we do that? Mr. Nielsen why don't you put in the record your answer to Mrs. Maloney's

Mr. NIELSEN. Thank you, Mr. Chairman. My answer is yes for the reasons suggested by Ms. Frawley.

Mr. HORN. OK. Ms. Goldman.

Ms. GOLDMAN. I think the greatest thing that Federal legislation can do in this area is to do what many of the people on the panel are doing right now. To make a decision as to where identifiable data is needed and where it's not. Right now, there's no requirement or no incentive to make that determination, but with a Federal law that provides for some very strict penalties and sanctions for misuse of information, I think there's a very strong incentive just by the fact of the legislation to use nonidentifiable data. Because then you take yourself outside the scope of the bill and you're not covered any longer. So I think that that is the key discussion that legislation will require and motivate.

Mr. HORN. Well, let me follow up now on what Mrs. Maloney's opened up——

Mrs. MALONEY of New York. Let me just——

Mr. HORN. Which is the next——

Mrs. MALONEY of New York. Should we just work off the existing——

Mr. HORN. Half hour, if we do.

Mrs. MALONEY of New York. This is a compliment to you, Mr. Chairman. Should we just yes or no——

Mr. HORN. You can have 40 minutes on that one.

Mrs. MALONEY of New York. No, no, no. Should we just work off the existing bills or should the chairman draft a new bill that does all this stuff? What do you think?

Ms. GOLDMAN. Well, we certainly welcome the chairman's leadership and involvement in this issue in the drafting process. I think there is certainly a partnership where Congressman Shays would be welcomed. I think it's important that some of the bills that have already gone through rigorous drafting and redrafting and have heard comments have benefited from that and it shows.

We're very hopeful that Congressman Shays' bill will continue to reflect the comments that we've all been making on it.

Mr. HORN. Well, I thank the gentleman from New York. I'll only yield myself 15 minutes, but let me round this out. Should there be a recordkeeping Federal office in the case of these codes of any experiment? How do we deal with that in your view, Ms. Goldman?

Ms. GOLDMAN. Well, very quickly, Representative Condit's bill does create an office of help information privacy. I think for the purpose of creating oversight and accountability, and monitoring the implementation of the law. I'm not sure that that's realistic in this day and age to talk about creating a new Federal agency, but what Vice President Gore and President Clinton have just called for is to create a person in each agency now to monitor privacy issues and to look at pending legislation. I think it's very important that there be an ongoing process of keeping track of how legislation develops, how it's implemented, making sure that the regulatory process is good and solid and that there's some oversight in the process.

Mr. HORN. Well, we don't have to develop a new agency for it. I mean, if you look at NIH research and the various protocols that are used in every university in the country in terms of consent, as

well as, in pharmaceutical and FDA. It seems to me that if the identification were needed, at least it would be in some place under proper procedures. For example, an experiment goes array over 25 years, and all the people that started it have long since disappeared, but then somebody realizes we had a problem with it, and we need to know who these people are. That's the question.

I'm just wondering what's a simple way to solve that problem?

Ms. GOLDMAN. Well, I think that would be very valuable, because part of the frustration and one of the biggest roadblocks right now to moving forward is we don't really have a very good record of current information practices where consent is required when it's waived under the Federal regulations.

I know that the National Bioethics Advisory Council is currently engaged in a project to look at how research is conducted and where informed consent is required. The human genome project is also very concerned with this issue. I think what would be helpful is to try to coordinate some of those efforts and to get one consolidated report.

Mr. HORN. Well, we could use the Institute of Medicine, the National Research Council, the National Academy of Sciences, National Academy of Engineering, if it was an engineering experiment; whatever will join with medicine.

Ms. GOLDMAN. And many of those bodies have issued reports.

Mr. HORN. Any other thoughts on what we should do to solve that little particular problem? Dr. Korn, you should be an expert in this area?

Dr. KORN. Mr. Chairman, I guess I've come to the point where I sharply depart from my colleagues' views on this. The way research is done, the locus or the site at which any coded material is secured has to be, I think, reasonably proximate to where the research is being done. In other words, if I'm an investigator on the faculty of Johns Hopkins Medical Center, then that medical center should be the site at which the keys to the codes are secured. And in all of the bills there's language talking about administrative, technical, and physical safeguards—that would be a requirement under every single bill, I believe.

It seems to me that one of the elements of such requirements would be how are you securing the code keys for individually identifiable patient information. I mean, it's a pretty straightforward thing. And it's just not practical to have a national office with hundreds of millions or billions of data elements that are going to be codes of all this research that goes on.

I'd also like to make the point that, and it gets back to an earlier question of the chairman, I think people are worried about the erosion of their privacy, but I really would ask you to consider where is the threat to individual well-being? It is not in medical research. That's not where people are being hurt. There's precious little evidence that people have been harmed from the last 100 years of medical research. A lot of evidence that a tremendous, a tremendous amount of good has come of it.

Mr. HORN. Well, don't you think that if one is in a medical research project on the point of which you made earlier, having to do with cancer, when that word gets out to the employer, to the insurer of that person in a patient situation, it seems to me there are

major problems. We find very autocratic decisions are made by employers, by insurance companies who want to get off the hook, et cetera. How do you solve that problem?

Dr. KORN. First of all, I don't think that the information that a patient has a disease comes from a research project. I think it comes from their clinical encounter with the health care system and the way we deal with medical care in this country is to have an insurance market. The insurance market underwrites, and the insurance market asks people for information if it's an individual kind of basis. The information that people are worried about is not coming out of research projects, Mr. Chairman. It's coming out of the ordinary transactions of health care delivery. I mean, that's where the diagnoses are made and that's where the information is then known to the payer.

Again, we're not dealing with cash transactions. We're dealing with third-party transactions and the information flows there. It's not coming out of the research labs.

Ms. FRAWLEY. I think it's important to point out, Mr. Chairman, that a lot of the information is flowing out of treatment and payment encounters. But I think the important thing that the committee needs to be aware of is the fact that we don't have a uniform national standard just on retention and destruction of individually identifiable health information.

I worked at Johns Hopkins. We had our medical records going back to when the hospital first opened. But again, when physicians retire or sell their practice, there are guidelines that are promulgated by State medical societies. But again, I've been in situations where I've had patients call me and say, "My doctor retired and I need access to my medical record. Do you have any idea where the record went?" So we have situations where we're sending out information to third-party payers for payment of a claim, sending out copies of medical records and I have no way of assuring afterwards if that record's been destroyed or has not been used for another purpose.

So, we have a problem just in terms of the notion of information practices that we're depending on ethical codes, guidelines promulgated by professional associations, and again, this shows no standard, here, in terms of how we handle information.

Mr. HORN. Yes.

Mr. KAHN. Mr. Chairman, with all due respect, there are laws which prevent insurers or employers from misusing information that they may have or discriminating against employees with that information. Basically, at the end of the day, an insurer, if someone expects them to pay for services, has to have some amount of records of what occurred, whether the services occurred, and what they were.

So, I think you really need to divide that process that insurers have to go through to pay for services from this other issue of the possible misuse of information. But the Health Insurance Portability and Accountability Act includes provisions that prevent discrimination based on the health status of an individual. And there are other laws that prevent such discrimination. I would argue that that's almost a separate issue from the issue of appropriate use of medical records.

Mr. HORN. Let's pick up on that point. To your knowledge, what are the best practices in America State law on the subjects we've been considering this morning? There's New York, California, they're usually ahead of the pact, Pennsylvania. What's the best practices we know of in this area? Anybody want to volunteer?

Mr. KAHN. I guess the National——

Mr. HORN. Do we preempt with Federal legislation whatever the State law is? Let's just start down the line here. If this bill is comprehensive, should we preempt State law?

Ms. GOLDMAN. As I said, Mr. Chairman, we are engaged in pulling together every State health confidentiality law. The challenge is it doesn't exist in one place in the State. So it might be in 15 different parts of the State's code. New York does have a comprehensive law. So does California. Minnesota recently passed health privacy legislation. A number of other States, Massachusetts not only has privacy legislation, they have a number of bills pending. The States have become much more active in this area, and as you've heard, that's of great concern to many people on this panel because it's made it more difficult to transmit information across State lines.

While I'm sympathetic to that concern, I think what we need to look at is where States have legislated in this area, and they've decided that citizens need certain kinds of protection. We need to be careful not to just wipe out those laws before we really know what they are, and we don't know yet what the State laws are in every single State in this country.

Mr. HORN. Well, give us your best shot in writing at this time in the record. Without objection, we'll be glad to put in your views on that. How about it, Mr. Nielsen?

Mr. NIELSEN. Well, I think——

Mr. HORN. Do we have a State that stands out in this area dealing with this issue?

Mr. NIELSEN. I can't answer that question, Mr. Chairman. I do believe, however, not only my company believes it, but the American Hospital Association strongly believes that if this thing is going to work it's got to be fully preemptive.

The situation that exists in this very area is an example of that. The health care delivery systems are a lot different now than they were 10 or 20 years ago. That's the reason I believe that we need preemptive national standards.

Mr. HORN. Yes, I didn't realize that if it is preemptive, Congress can also write-in, if there is a stricter law that can prevail over the Federal law.

Mr. NIELSEN. Yes.

Mr. HORN. We've had that fight with the Department of Agriculture. We accused them of being dominated by Tyson's chickens because they're sending frozen chickens into California, where there's a much higher State standard, as there often is in the case of California and New York. Agriculture says, oh, sorry, the Federal law applies which is a very weak law in frozen chicken. If you want to get botulism and everything else, just follow the Federal law, since they won't let us use the California law, et cetera.

But I think that's something we can work out.

I agree with you that most people in this interconnected society, if you will, no matter what we do, should be operating from one set of basic laws, if we can possibly do it, and it does not prove to be unreasonable, to the average person.

Dr. Korn, any thoughts on that?

Dr. KORN. As I've said, Mr. Chairman, we strongly support a strong Federal preemption, both because of the realities of our consolidated health care system that we've created and the reality of how the retrospective research that I referred to works. The archives exist in every State in the United States, and in order to have uniformity of rules and regulations that deal with the security and with access to them, it seems to us it would make much more sense to have an appropriate law at the Federal level that was preemptive.

Ms. FRAWLEY. Since our members work in all of the States, right now we're dealing with 28 States who have statutes on patient access, fairly uniform in their approach. Thirty-four States have statutes and regulations on confidentiality. Again, a variety of approaches there. Nineteen States have laws on genetic privacy.

We also have Federal alcohol and drug-abuse regulations which govern disclosure at the State level. We also have concerns in terms of the Federal Privacy Act which could also govern disclosure. We did have two States in the mid-1980's who passed the Uniform Health Information Act which was an attempt in the 1980's to get uniformity among 50 States. Montana and Washington State passed it. The problem that you have is when you look at it 10 years later, there's an aspect of the health care delivery system that that legislation didn't contemplate.

Just looking at the entire mix we're dealing with right now, I could not point you to one State that has a comprehensive law and say this is the model, which is why we're sitting here kind of deliberating on what's the best approach.

Mr. HORN. Any thoughts, Dr. Harding?

Dr. HARDING. I think the States are churning right now, trying to come up with something. I think one of the States to look at would be Massachusetts, who seems to be in the forefront of this whole issue. I would like to say South Carolina, but I'm afraid I can't.

Mr. HORN. OK. Mr. Kahn.

Mr. KAHN. I think the point here is that in some ways I see you starting from scratch, and you do have to have a uniform set of rules otherwise it's just going to be impossible to administer, at least from the standpoint of insurance or managed care plans, impossible to administer the kinds of information that we have to deal with.

Mr. HORN. Dr. Andrews.

Dr. ANDREWS. I could not point to a State that stands out as a model of what we should do. But I think we could look at the Minnesota experience as an example for a new type privacy law that requires informed consent for any use of information, even for research and archival records have been required and is having a tremendous effect in impeding the progress of research.

The Mayo Clinic, which has a great history of excellent research that's benefited hundreds of thousands of millions of people over

the decades, has the resources to retroactively obtain consent on hundreds of thousands of patients—great expense. I suspect that the average institution would not be willing to invest that kind of resource in getting consent. When, in fact, their experience is that 97 percent of the people they contact are giving consent.

Mr. HORN. Let me ask you something on this aspect of privacy. Are any of you familiar with the European community European unions' views on the privacy situation, and the proposal they have adopted in their Parliament which will apply in October of this year? Anybody follow that development and what does that mean for the medical health care records in this country, whether our people are traveling in Europe or whether a European is traveling and wants their records?

Ms. Frawley, you seem familiar with it.

Ms. FRAWLEY. Yes, we've been tracking that for a number of reasons as you just mentioned because of the concern in terms of the impact that would have. As far as Europeans who come to this country for health care, obviously, in order to get access to their information, we would have to get an authorization.

I think the bigger concern is companies who are involved in clinical information systems or involved in global research and there are concerns there that if the United States doesn't have strong data protection laws in place, that that could have an impact on some of the companies who do business internationally. So there are some concerns there.

But I think in terms of patients in treatment situations, I think there is less concern as much as it is in terms of some of the research that is being done internationally, and also companies who deal with information systems in terms of any transfer of data.

Mr. HORN. Anybody else involved with that? Yes.

Ms. GOLDMAN. If I can just add to what Ms. Frawley has said. The European Union directive is very clear that information on EU citizens cannot be transferred to a non-EU country such as the United States unless that country has what are considered adequate levels of protection. Adequate compared with what the EU Director requires, and it requires explicit informed prior to disclosure.

Now, one of the things about the EU directive, is that it allows for the EU to look not only at the laws of that particular country, but also at certain kinds of practices and codes of conduct in State laws. But the number of people from the EU have been very clear that they're concerned about the United States' lack of medical privacy law because it's such a gaping hole when compared with the rest of the body of our Federal privacy law.

Mr. HORN. Anybody want to comment? Anybody else? We're going to be looking at that issue very closely. A number of us have met with the leadership in Poland and in France, where we just happened to be, to discuss this situation. It does hold a major problem, not only for individuals, but for subsidiaries of American corporations in Europe and subsidiaries of European corporations in the United States. So both the International Relations Committee and this committee will be looking at it.

Law enforcement access—that came up with several of you. Are most of us feeling that that should be through a neutral court. Or, for example, if there's a murder or a suicide or whatever, and the police chief has got a group of detectives trying to solve the case. He phones up the hospital and says I understand so-and-so and so-and-so. Should that file be turned over? What is your thinking in that area, and have any of you had to grapple with it in any of your member institutions that are part of your organization? How about it, Dr. Andrews?

Dr. ANDREWS. Fortunately, I haven't had to grapple with that. And in terms of PhRMA, we do not have an officially adopted position regarding the law enforcement access.

Mr. KAHN. We don't have an official position, but I think courts ought to make the determination here.

Dr. HARDING. Yes, the probable cause.

Mr. HORN. With psychiatric files, would you prefer the court in that?

Dr. HARDING. Prefer that the court be involved.

Mr. HORN. A judge required. In other words, the department of police or the sheriff's office would have to go, somewhat as we do now, tapping wires and FBI requests, to a Federal district judge. Well, would it be sufficient if they are seeking those files for State judges to make that decision or would this all be dumped on the Federal judge?

Dr. HARDING. No, a State judge would make it, as it is now.

Mr. HORN. OK.

Ms. FRAWLEY. Currently, most States have laws which require health care providers to report situations involving traumatic injuries, such as homicide, suicide, arson, child abuse, and child neglect. There is a responsibility that when a patient presents an emergency department that providers are required to notify the local authorities.

My concern is that when the detective comes into the emergency department to interview the patient that the hospital called and appropriately notified that we not have detectives on a fishing expedition to find out who else is in the emergency department or what other people are there seeking care for. I think that we definitely have a situation where any law enforcement access will need to have a warrant or a court order.

There are too many days where people are showing up and flashing a badge and providers or their staff are standing there trying to decide whether or not they need to provide access to a medical record. Certainly in terms of fraud and abuse use investigations, there are venues that can be obtained to get a warrant or a court order to have access to records.

But I think that we need to tighten up that area.

Mr. HORN. Dr. Korn.

Dr. KORN. Yes, our association strongly believes that law enforcement access to identified medical records should require a court order.

Mr. HORN. Mr. Nielsen.

Mr. NIELSEN. Mr. Chairman, I have a little bit of interest in this and some expertise. I've been a prosecutor and a law enforcement official in my career, and I certainly understand and appreciate the

needs of law enforcement to ferret out fraud and abuse and to solve crime. However, I think a lot of the discomfort in this area arose out of Secretary Shalala's recommendations. In particular, the implication that there ought to be left in place, the ability of law enforcement officers to obtain medical history information simply upon request, when they say they need it. That has, of course, bothered a lot of us who believe that there ought to be some sort of court oversight with respect to those seizures.

Now, I don't want to give a lecture on criminal law and criminal process, but there is a difference between the obtaining of a search warrant and the obtaining of a subpoena, because there are various degrees of court oversight, certainly.

The American Hospital Association's view is that certainly the traditional elements of probable cause ought to be present when officers are seizing records pursuant to a search warrant. And that other types of seizures ought to be at least completed with some form of court oversight, and this is either a subpoena or otherwise that does have the advantage of at least conferring jurisdiction on courts, so that those particular requests can be reviewed for overbreadth and materiality.

Mr. HORN. Ms. Goldman.

Ms. GOLDMAN. I completely agree with my colleague, Mr. Nielsen. I think that we must incorporate a constitutional principle in a Federal privacy law that would be, at least, as strong as what we currently give, as I said earlier, to credit records and video rentals, as in financial records. I just don't think there's any justification here for sidestepping this issue.

Mr. HORN. Thank you.

I now yield 15 minutes to Mrs. Maloney.

Mrs. MALONEY of New York. I thank the chairman.

I'm sure all of us respect privacy. But the problem is when some people don't, and use it to their own advantage or abuse it, and it seems to me, how do you get to that point to protect individual privacy? And I give the example that was reported in the press of some doctors selling medical information to pharmaceuticals or drug people who want to sell drugs, so that they'd know where they could go to sell the drugs to these particular people. I use that example. Do you recall reading that one or seeing that one? Would anyone like to discuss that one? How would you keep that from happening? I'm just using an example of an abuse that was made public.

And then another abuse. One of our colleagues was in a tight race and her medical records appeared on the front page of the New York Times in a very detrimental way, a very unflattering way. Obviously, it was the responsibility of the insurance companies and the hospitals to keep that secret, but they didn't and it ended up on the front page of the papers. And that's very troubling to a lot of us. Can you comment just on those two examples and how you would have prevented them?

Ms. FRAWLEY. The first example that you pointed out is the use of data for commercial or marketing purposes. And our association has issued a position statement on that. We are troubled by the fact that there are providers or other organizations who receive health information, who do not believe it is unethical or inappro-

priate to use information for commercial purposes. We see that as a prohibited activity. I mean, that that should not be ongoing.

Mrs. MALONEY of New York. But isn't it prohibited now?

Ms. FRAWLEY. No, it's not. In most State laws, there's no prohibitions. And on top of it, if there is a breach of my personal privacy or confidentiality health information, in many States I don't have a civil right of action. I can't even bring you into court and obtain a remedy. So that's the biggest problem that we face right now.

I think most of us are in agreement that any legislation has to have strong civil and criminal penalties. Because right now, most States do not have those protections in place. The instances that we point out or that are reported in the media, most of these patients have no right of redress. There is nothing that they can do.

Congresswoman, having worked in New York City and being familiar with the particulars of her case, the situation that you're dealing with is that you are really putting a lot of trust on your health care provider and in turn, we proffer testimony that we have to send information out for a variety of purposes. And oftentimes, there is little control after the information——

Mrs. MALONEY of New York. But to use her particular case, of course, everyone said, we don't know how it happened. So it was absolutely——

Ms. FRAWLEY. Well, part of that is because there was no accountabilities built into the system. That's one of the things that I think is important about Congressman Shays' draft, is that any organization that collects, stores, transmits, maintains, handles information has to have accountabilities.

I think that's really important part of any legislation because so much of the health information that we deal with in this country is out-sourced to third-party vendors, and we have transcription that is being done outside the care setting. We have people who are handling patient records. We have clearinghouses who are processing health care claims. These people are in a contractual relationship with a provider. And if you look at most of those contracts, it probably doesn't even address confidentiality or what types of information for security practices there need to be in place.

Well, it's really raising the bar for everyone who is part of the health care delivery system or handles health information. Unfortunately, the person who is least informed in this whole relationship is the patient.

Mrs. MALONEY of New York. Anyone else like to comment on those two particular examples and how we would stop them?

Dr. KORN. It's my recollection, and again, I can't keep precise track of these various bills that have passed across my desk, but at least a couple of them explicitly make it a Federal crime to use identified patient medical information for commercial purposes.

It seems to me personally, that that's a very good provision to put into any Federal privacy legislation.

Mr. NIELSEN. Let me just respond to that, Representative. And it comes back to two things that I think have been said previously. Dr. Andrews, I suspect, framed it about as well as I've heard it put, and that is, these kinds of examples have given the impression to the general public that their medical records are, in fact, not safe and they are being treated in a cavalier fashion, and is susceptible

to these kinds of terrible abuses. I think it needs to be made very clear, we're not going to prevent totally these kinds of things occurring in the future, no matter what law we pass.

The issue is the integrity of the people we hire and that we deal with, to deal with these records. Things like that, even if we have a Federal law or State law, are going to happen. But there are things that we can do to try to prevent them.

In our organization, for instance, our employees sign a confidentiality agreement; they go through an extensive training program as to what they can and cannot do with information they receive. Not everyone is cleared for access to certain kinds of information. And we have a fairly sophisticated ability to track access to computerized record systems, and those are audited periodically. So we can determine if persons are having unauthorized access.

Mrs. MALONEY of New York. Now that's an important point, to track the access.

Mr. NIELSEN. Yes.

Mrs. MALONEY of New York. As I said, I truly believe that most people in health research, delivery, insurance, all of them are highly reputable, wonderful people who are concerned about doing a professional job. But there are people who abuse it, as you said. Do you think you should be putting in the bill, some way of tracking access so that you can find these people? Or would you just leave that up to the individual companies or——

Mr. NIELSEN. Well, I think the bill suggests that that be part of these regulations that will be promulgated dealing with electronic transfer of information.

The fundamental aspect of all of this and I suspect the tail end of it is, is that we ought to punish people severely for these kinds of breaches of confidentiality. And I think——

Mrs. MALONEY of New York. But you can't find them, because the system isn't such that you could find who's leaking it.

Mr. NIELSEN. Well, I'm assuming you can identify them. They ought to be punished. That is the deterrent.

Mrs. MALONEY of New York. Anybody else like to comment?

Mr. HORN. It's 15 seconds, if I might, on Mrs. Maloney's point. It's a very crucial one. She and I sat through a lot of this testimony when Mr. Condit was chairman of the committee. There were some really horrible stories that came before us. People that might have just been disgruntled employees, sort of take the file of the mayor with them on their way out of the office.

And the way hospitals were handling records, wasn't exactly secure, shall we say. That would be the "understatement of the year."

Then, we had one of our colleagues records revealed in the midst of the day, practically in the midst of the political campaign she was in. So, there are a lot of these examples. Mrs. Maloney's made some important points there.

Ms. FRAWLEY. I just want to comment on that. The National Research Council study that was published last year, we spent 18 months looking at health care providers and other recipients of health information and if you look at the recommendations of that report, it talks about the fact that organizations need to put in place, strong organizational and technical practices to safeguard information.

Unfortunately, when we were making site visits throughout the United States, we were not able to identify one model organization. And the report lays out what we thought the important components were, but we could not look at an organization and say, here's a model organization that incorporates all the practices that we think are important. Certainly, what Mr. Nielsen points out at Intermountain is very important. You need to have a record of access. You need to know what employees have been credentialed and are accessing a patient's information. You also need to have disclosure logs so that you know when you're sending information out to a third party where that information is going. More importantly, the patient should have the right to know how their information is being handled.

So, there are hospitals now that are piloting projects where a patient can log on and actually know who has had access to their health information, and I think that's very important.

Mrs. MALONEY of New York. And then to get to the area that has been very critical as really unworkable in the health care provider industry, that of patient consent if their information is used. If you have patient consent, doesn't that build in accountability? In other words, take the Velasco—give the example of her information is out there. Well, how did it get there? No one knows. But if you have patient consent built in with the doctor, there is some accountability, somebody caring that this does not get out because their name is on it in a sense, too. Do you see what I'm saying?

Why is patient consent not workable? Many people say they believe the intent of it, but they say, that in the practice it's just not going to work. Why wouldn't patient consent be—I would consent to have my medical records used for research. I wouldn't consent for them to be put on the front page of the New York Times, but why is patient consent such a bad thing? It seems to me that that helps build in a roadblock. Maybe you don't get your research as fast as you want it, but at least there is some type of protection to the abuse of the individual.

Ms. FRAWLEY. Well, I think all of us have testified that patient consent is important. I think the important thing that most of us pointed out is that patients are generally not informed. So, I think the important thing is that if you're asking the patient to authorize disclosure of information for treatment or payment or health services research, the patient needs to understand. Most patients don't understand when they are authorizing disclosure information for payment, how much information may be disclosed.

Or, I say I'm willing to have information released for health services research, understanding the implication of that decisionmaking. I think the problem that we have is that a lot of times, if you look at the authorizations that are currently in use—you know, I sign up for insurance and I have a little blanket statement saying I authorize disclosure of my information. I think we need to do a little bit better job up front, educating our consumers, so that——

Mrs. MALONEY of New York. I think you raised a very important point.

And if I could then go to Mr. Kahn who is representing the insurance industry.

I've raised it. I represent a number of important insurance companies in this great country of ours, and they assure me that all the information is confidential. How is confidential? Why not do what she said and spell out how our information is going to be used?

I have an insurance plan. So I always sign to be reimbursed in my insurance. I always wonder to myself, I don't understand who else is looking at this. Would that be such an onerous requirement to ask the insurance companies to sort of say, when you check this, this means the reimbursement office will see it and maybe whoever else has to see it? But it's not going to research. It's not going to here; it's not going to there. It's not going to be sold. Would that be an onerous situation?

Mr. KAHN. Let me say two things. First of all, I think that one has to be careful, with all due respect, to make policy based on hypotheticals or anecdotes. The fact is that insurance companies and health plans process today billions of medical claims for services, and you don't have rampant release of health information. Sure, the examples you're bringing up are horrible, but there is not study that I have seen that shows a consistent pattern of release of information that people would not want released on any basis.

Mrs. MALONEY of New York. Well actually, Mr. Kahn, the two examples that I gave did not involve the insurance companies at all.

Mr. KAHN. I mean, just in general. Not that privacy shouldn't be protected or confidentiality isn't important, but my point is that currently, in the current environment, as much as we're lacking in rules at the State and Federal level, there are not patterns of abuse, although there are, obvious, pockets or examples of abuse. So, I think that's important.

Mrs. MALONEY of New York. I'm not in any way trying to pick on the insurance companies. My father was an insurance agent, so I mean, I'm very sympathetic to the insurance business. But I want to understand it better. And it's a friendly question that I'm trying.

Mr. KAHN. No, I understand.

Mrs. MALONEY of New York. So, I just want to ask you, when I or Mr. Horn or any of us, sign our insurance form when we're in our doctor's office, who sees that and how is that information contained?

Mr. KAHN. Well it goes to the company and there will be a claims person who will review the claim and if there is some question, it will go to the medical director or the medical people.

Mrs. MALONEY of New York. But then, how is that contained and kept confidential? Can anyone buy that? Can anyone see that?

Mr. KAHN. No, every company has its own computer systems with its own confidentiality rules. And that is only for the use of the company.

Mrs. MALONEY of New York. Only for the use of the company?

Mr. KAHN. Right.

Mrs. MALONEY of New York. So, when people sell lists of who's taking what medications, it's not coming from insurance companies, it's coming from doctors directly? That's my question.

Mr. KAHN. It would be or other kinds of entities that have information. I mean, as was discussed today, there are a host of entities

that have information about you. I mean, there are drug stores that have information about you, as well as doctor's offices and other kinds of providers of services.

Mrs. MALONEY of New York. Would it be helpful, to sort of, bring it down to the level the man and the woman on the street understand. There is a tremendous fear over medical record abuse. I think a lot of it is really justifiable, given the fact that it has been abused, not by reputable people, but by some disreputable people. Would it be too onerous to ask whether your pharmacist or insurance company or doctor to have plain English saying, this information is being used x-y-z only, and it's a Federal offense to use it any other way? It just sort of brings it down to what people can understand.

Mr. KAHN. Well I think there does need at some point in the process, to be permission given. In the case of claims of other kinds of insurance matters, there is permission given for the insurance company to use information that people want services paid for.

Mrs. MALONEY of New York. But it's given, my point is, it's given to the insurance company to have it paid. But then, the question is, what happens to it then? With computer systems and everything else, it's so easy for people to get access to that information. I guess what we're asking for is how do we not only build in clear directions to people that are in the business to be confidential about it, but how do you prevent people who may want to abuse the system from not being able to abuse the system.

Mr. KAHN. There's a model in the Shays bill where there's certain kinds of use of information that is prohibited because it's considered inappropriate or misused. I think using information for commercial purposes, in our case, other than simply ensuring that the services were provided, and are covered under the product that that person has, the insurance policy that person has, it seems to me that's perfectly reasonable.

Mrs. MALONEY of New York. Well then, let's take it another step. Not only are you barring it from commercial purposes, but maybe you might outline exactly how it is going to be used and if it is used any other way, then it has to have the patients consent. I think that's something people could understand. Then how do you define commercial purposes? You see, what's commercial purposes to us, there may be another definition in another State that exempts it.

Mr. KAHN. Well, that's why you need uniformity in a Federal set of rules, both laws and then regulations to back those up. And then presumably, there would even be a court history once those laws are put into effect.

Mrs. MALONEY of New York. Well then. Yes, sir?

Dr. KORN. Let me comment about that. I think the intent of the bills that I've read is to require organizations or institutions that are dealing with medical information, that they must have, the language I believe is, administrative, physical, and technical safeguards in place that define their security practices and assure to the best possible level that those practices will be adhered to within their organizations and institutions.

The consent issue which has its own independent merit in discussing, of course, is not really the key to this, I don't think. Be-

cause, if one wanted to make process maps, that's another popular thing that people like to do, the process map that would follow an item of medical information that's taken in the course of a clinical encounter, let's say, in a hospital or clinic setting, has probably got hundreds of steps in it. That is the actual fate of that item of information as it flows through the system, both in the management of the patient in the particular instance, the recordkeeping that is done along the way, the distribution of information for purposes of payment, oversight processes, and many of the bills actually list these processes under their definitions.

Mrs. MALONEY of New York. But, I think the problem is that the hospital that Mrs. Velasco's went to, to give you an example, I'm sure had administrative, technical professional guidelines to maintain the patient confidentiality, and they didn't. So, the times that you do see it, is when someone deliberately wants to abuse the system. Most of our medical insurance professional health care are high-purposed people. It took them many years to get to their positions. But, it's not like we have to tell hospitals to be professional and have good systems. I think every hospital thinks they're professional and have good systems.

It's how do you build in another link that is an extra protection for a patients records? I guess maybe the civil penalties is the way, but obviously there are a lot of professional—I think every hospital in New York City is a very professional hospital. It's among the best in the country. Of course, I'm prejudiced. Yet, it happens that the files are abused in these hospitals, for whatever reason. Because they want to hurt a person politically, or for whatever, they're abused and they can't figure out who did it.

Dr. KORN. I think, first of all that having a Federal law that establishes a threshold of expectation in the way of standards is an excellent idea. I think all of the institutions could be better than they are, probably.

I think that if you're asking me, I'll give you a personal answer. Others may have their different opinions, but if you're asking me personally, whether there's ever going to be a system so airtight that each contact with an item of medical information is going to leave an indelible fingerprint, so that, if something unfortunate happens, somebody's going to be able to go back there and recreate the history of the information and say, it was John Smith who called the New York Times about so-and-so's medical record, I'm not sure if I'm going to live to see a system like that.

I do think, as Ms. Frawley has mentioned and others, like the NRC report on the electronic medical record, there is a very extensive set of recommendations that become feasible with electronic information that are not feasible with paper information. I think that the members should keep in mind that implementing the level of computer-based information handling and the system of security of that information that people dream of is going to be a very major, expensive process for all who are involved in handling medical information. That is not a reason not to promote that it be done. I'm not arguing that.

But I do think that you should be sensitive to the fact, that one is talking about vast capital investments. I know of one system in a city near New York, but it isn't quite in New York, where a major

academic health center has budgeted already over $100 million to try to develop, what they believe, is the standard of electronic medical information capability that they wish to have.

Those are very, very large sums of money. And you've got to be sympathetic to the fact that not every organization that handles medical information is going to have the financial capacity to run out the next day and implement that kind of system. There may have to be some kind of Federal system on implementing some of the standards produced under such laws.

Mrs. MALONEY of New York. Are there any other comments? And I have one last question that goes right to the heart. Anybody else want to comment on that?

Dr. ANDREWS. I wanted to make a brief comment. I agree that there is need for adequate safeguards and penalties for those who abuse the system, because you can't set adequate controls to prevent abuse.

But I'd also like to go back to your question about consent. I think we need to be very clear when we ask for consent and when we don't. For example, I think we've all said that for the use of archival records that do not contain identifying information, obtaining consent would be inappropriate and would serve to impede the progress of research if we allow people to opt-out of important, large studies where it's important to have accurate and complete information of large populations of people monitored over long periods of time.

Mrs. MALONEY of New York. Anyone else? Yes.

Dr. HARDING. I think if you sign a consent, my assumption would be that the minimal amount of information necessary to get that treated and paid for is what would go to the insurance company, the minimum amount. Instead of asking for the medical record for the payment of that. That's a problem. If you get more and more information in one place, that that becomes more and more valued by crooks, so-to-speak who would like to get where the gold is.

The other thing I'd just like to mention is that the Congresswoman had her record partitioned for sensitive information, that information may not have gotten out in her case.

Mrs. MALONEY of New York. What do you mean partitioned for sensitive information? What do you mean?

Dr. HARDING. That there are certain medical conditions that are felt to be more sensitive than others, and that if there is an electronic partition of the medical record, it would leave regular medical record issues or regular medical problems, and then have those that are especially sensitive—the ones that are often mentioned are mental illness, ob-gyn issues, infectious disease issues, genetic issues, and they are, in effect, a black box in the electronic medical and only can be obtained with special keys, then that would prevent some of those kinds of Congressman disclosures that happened in the past.

Mrs. MALONEY of New York. Mr. Kahn.

Mr. KAHN. Let me add that we do have to be careful that there is in managed care, a great deal of utilization review and quality assurance that requires having information about services provided to people both to prevent fraud and abuse and to improve quality.

If you just look at the new Medicare-Plus Choice requirements that are going to be put in place for Medicare beneficiaries that sign up for private plans, there's a tremendous amount of information that's required of plans to collect in aggregate on the beneficiaries they're providing services for. So they can assure that there's quality care being provided.

And beyond that, there is legislation now being considered by the Congress that would make even further requirements on health plans. So, I think we do need to be careful here that a lot of the information that health plans, and insurance companies, and managed care companies have. There is an expectation that they will use that information appropriately, for utilization review or quality assurance purposes. To place too many limits on that, will really upset the plans that cross purposes with other public policy, that's requiring them to collect information so that we know better the quality of services that providers are providing.

Ms. GOLDMAN. Can I just add one last thing to clarify. When people talk about what are the problems out there currently, we have much more than anecdotal evidence, and I've included much of this in my statement. But we have polling data that suggests that one-quarter of the American public withholds information from their doctors and from their health plans because they have suffered some kind of inappropriate use.

One-third of all Fortune 500 companies in this country look at people's medical records in making promotion and hiring decisions. They often get that information from the health plans who see the employer as the customer to whom they owe a duty and not the patient. So when the employer asks who is paying for the plan, when they ask for data, it is given to them.

Many people that I have talked to within the health plans would like some kind of restriction on that, but there's a competitive environment right now that requires that they respond to requests from employers for information. So, no matter how many stories we list in our statements, the truth is we are way beyond an anecdotal situation. This is a serious, serious problem. Because we're dealing in an environment where there are no rules. There are no limits.

Mr. HORN. I thank the gentlewoman. That was a very interesting 25 minutes of questioning, and I enjoyed it.

I've got only a few other things here, and then I will be glad to yield back to Mrs. Maloney, but I want to make sure we have a little further discussion of them.

We mentioned the segregation of records, in response to one of Mrs. Maloney's questions. We discussed mental health as an obvious one. There would also be genetic makeup. What are some other areas that might be up-front segregated under some better privacy protection that perhaps we've seen? Mr. Kahn.

Mr. KAHN. I guess, Mr. Chairman, I would ask if you are going to write legislation to protect the confidentiality of records, why should these particular areas you mentioned, be considered any different than others? I mean, you're developing and talking about legislation that would prevent abuse to prevent misuse of information so, why would you want to partition off this information that is part of any record?

I mean, let's take the mental health, for example. There are many pharmaceuticals now, and more and more as time goes on, pharmaceuticals that are given in mental services. Why should that information be partitioned off from other records when it could be critically important to other professionals who are providing care to a particular individual, other than the psychiatrist?

I just think that you're making an assumption which I think you should question, about whether or not there is need for partition, if you're going to set a baseline of rules for all information.

Mr. HORN. It's a good point and we'll take it under consideration. Yes, Dr. Harding.

Dr. HARDING. I would agree with those comments in a perfect world. But, if the Congresswoman that we are referring to, had twisted her knee and had been in the hospital for a few days, it wouldn't have made front headline news. We have a special issue that people are very sensitive about, and which there is stigma, and prejudice, and so forth.

Mr. HORN. It's the "ego-son phenomenon."

Dr. HARDING. And so that's why it was front-page news, and it shouldn't have been. It shouldn't have even been covered because it was a private issue. But because it is that issue, just along with infectious disease and other things that happen, reproductive rights, those things get put on the front page. And we have to address reality, that they are special.

Mr. KAHN. But if I could add. The reality is that many urologists now are going to know whether or not someone takes Viagra and that could be just as incriminating as anything. So, I think to try to partition this off is going to be very limited. You can't do it.

Dr. KORN. I'd like to say for the record again that we're very opposed to any proposals to segregate the medical record. We think all of the information is sensitive, and it all ought to be kept to a standard. I said earlier that every disease is sensitive to the person who has that disease, and we all encounter that.

Let me just give you an anecdote—a hypothetical. We're in an era now where psychiatry is moving more and more into a capacity to use drug medications. They all have side effects. Is a patient well served that comes into emergency room in liver failure which is potentially a fatal disease, where she doesn't want anybody to know that she's been seeing a psychiatrist. And the psychiatrist has not ever had in the record that she's been prescribed with a potent psychotropic drug that happens to have a side effect that wipes out her liver. Who's being helped by that kind of a strategy?

Ms. FRAWLEY. I think it's important having managed record systems. There is really no way that you can partition or segregate information without inadvertently breaching the patient's confidentiality. I mean, I managed psychiatric records and what we did was, we had the main medical record and then on the folder, we told you there was a separate record. You didn't have to be a rocket scientist to figure out that there was a psychiatric record.

As Dr. Korn points out, partitioning information and creating subrecords or subfiles are putting providers at risk. We have documented instances of people having adverse drug reactions because the physician was unaware of the fact that the patient was receiving treatment for other conditions. And the problem that you have,

as soon as you segregate or partition information, keep in mind that most of our medical records are still paper-based.

Unfortunately, we're not at the level of Intermountain. I mean, most of our providers, and we have a lot of physicians that don't even have computers in their offices. We're still dealing with a traditional paper-base model. And the problem that you have is that if you're starting to segregate information or take pages out of charts, you're going to really wreak havoc on the quality of care. We really have to address the issue underlying all this discussion, which is the discrimination by insurance companies and employers against individuals.

That's a whole separate argument in terms of this particular issue. But asking people to try to segregate information, creating subfiles, it would become unmanageable. Having worked at Hopkins where I had a main medical records department and 13 satellite record rooms, and a psychiatric record room, I could never for sure guarantee anyone when they sent me a request and said send me a copy of the patients medical records, that I ever had the entire medical record, because there were records all over the place. And that's not the way to render health care in this country.

Mr. NIELSEN. Mr. Chairman, may I just get some clarification on the scope of your question or the intent of it? Are you suggesting segregation in terms of how we would construct a statute? Or, are you suggesting that this is something that would be done internally by the providers?

Mr. HORN. The question would be, and it's been mentioned by some of you, the degree to which some types of records really need to be private: To put it in a simple layman's way, so it gets out about your broken knee. Or you had your tonsils out. But then the question is, of course, if somebody's playing political games, they would be saying, why are her/his records so damaging to them in terms of health, that they keep them in a special lock-up room. I mean, you'll always have that with the idiots that sometimes get into political campaigns.

What we were thinking of is what a lot of people are worried about, the genetic situation, where employers could say, "jimminy crickets." Or insurers, who are the main ones here, could say, sorry, it looks like your going to drop dead at 45. You've got a long family of this, genetically, and we don't want to insure you. A lot of people don't even want to know about their genetic charts but, somebody might be requiring whatever was done in relation to something completely different. And it happened to slop-over into a number of other things.

So, I'm just trying to explore what your thinking is, in terms of best practice.

Mr. NIELSEN. I think, I agree with what my colleagues have said about the dangers of this notion of segregation. However, it is possible to some degree to limit the ability of the provider of the community to have access to certain sensitive kinds of information. For instance, not every nurse in our system has access to records in the psychiatric unit; that is blocked. And unless they have special codes that allow them access, they can't get into it.

Those kinds of procedures internally are certainly possible. I guess the reason for question relates really again, to the preemp-

tion notion. Are there certain kinds of medical conditions that we ought to accord special protections, segregate them out for additional statutory protections or not? In our view as a hospital association is clearly, no. We ought to have a national standard; we ought to be able to know, with certainty, on a national basis how we protect all forms of medical information and medical records. For those reasons, we would urge care in trying to segregate out these conditions. I mean, where does it stop?

Mr. HORN. Well, here's another example, in a typical hospital records room. Let's say Dr. X, who has nothing to do with the patient, not doing anything in that area, not even related to what the patient's had under terms of operations and all, and yet, he's just a curious guy. And he's sort of one of the men about town or the woman about town. And he'd just like to know what's going on, and by the way, Joe, do you know so-and-so's had this happen? I don't know why that doctor needs to have access to that file. I just wonder what do the hospitals of America do to cut down the level of gossip in a particular city about one's health situation?

Mr. NIELSEN. Well, I could tell you that that example probably occurs. And in response to Mrs. Maloney's query, I indicated that's why you need some sort of tracking mechanism to determine who, in fact, is having access to this and why.

Mr. HORN. Well, they certainly should sign that they had access to the file.

Mr. NIELSEN. Surely. That's the paper aspect. I'm talking pretty much about computer access. There ought to be some way you can get back in and track who is having access to that. If people have no business looking at it, and that can be determined quite easily as you review the audit trail, then there ought to be something done about it. And that may be dismissal from a medical staff, some other type of penalty internally, or as the bills provide, sometimes criminal sanctions and certainly civil sanctions as well.

Mr. HORN. Of the hospitals with which you're familiar, and I'll ask this of all of you that represent hospital associations, is it common to use the Social Security number, all of it, or simply the last four digits plus a birthdate?

Mr. NIELSEN. I can tell you what we do, and I think it would be very common with most personal identifiers. We do not use Social Security as a personal identifier. In our system, patients are assigned a unique code that has no relation whatever to the Social Security number. I think that would be fairly common with——

Mr. HORN. Is it a numeric code, or an alphabetic code, or a mix thereof?

Mr. NIELSEN. You know, I don't know how it's formulated, but I do know that it's completely unique to the individual.

Mr. HORN. So when you are added into that system, they have the next number up and it's yours and that's somewhere coded in with your name, I assume?

Mr. NIELSEN. Well it may be. I'm just not sure how that's assigned.

Ms. FRAWLEY. Most hospitals in most physician offices use a unique identifier which is generally numeric and typically most organizations have a master patient index or a directory service

which would contain the name of the patient, their date of birth, other demographic information, last dates of treatment.

So, the main thing that you want to do, when a patient presents for care, is to always be able to link prior records of treatment. So that typically organizations have a unique record system and a unique numbering system. And basically, the number would not mean anything else to anyone outside the organization. There's no intelligence in the number. So organizations do not use Social Security numbers as their identifier.

The concern now is that with the Health Insurance Portability and Accountability Act, there is a mandate for the Secretary to adopt a unique health identifier for individuals. And the concern is people are worrying about the use of Social Security numbers as an identifier for health information.

Mr. HORN. Anybody else want to comment on this point? If not, let me move here to Dr. Andrews. The concern was brought up earlier that some individuals that have a particular type of case, their names would be turned over to pharmaceutical companies to followup on. Now, is that common practice in the pharmaceutical industry?

Dr. ANDREWS. I think you're referring to the CVS example. Someone else made the point earlier that that was a misquote in the Washington Post. The company never obtained any identifying information about individuals.

Mr. HORN. Well, I'm looking here at Ms. Goldman's testimony where she cited a few examples on page 3, "and medical marketing service advertises a data base available to pharmaceutical marketeers which includes the names of 4.3 million people with allergies, 923,000 with bladder control problems, 380,000 who suffer from clinical depression."

Then, a recent article discussing new demands for health data explained that data can come from a variety of sources, such as pharmacy and/or medical claims, patient or provider reports, and patients' charts. At PCS, and this is translating data and useful information to the involving role of PBM in the drug benefit trend, and it says "data can come from a variety of sources, such as pharmacy and/or medical claims, patient or provider reports, and patients' charts."

At PCS, the Outcomes Research Group has on-line access to 700 million pharmacy claims, which represent the past 25 months of prescriptions filled. The information on a prescription becomes available on-line within 48 hours after the pharmacist dispenses it.

Then another example, an Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol. This is from the citation, "many can hear what you tell your doctors: records of patients are not kept private," Orlando Sentinel, November 30, 1997, page A1.

So, I just wonder what the reaction of the pharmaceutical manufacturers and researchers is?

Dr. ANDREWS. I can't speak to the specific points here. What I can say is that from my knowledge, within a pharmaceutical company, companies do not obtain the list of names and addresses from those kinds of sources.

Mr. HORN. Well, if you could get us an answer from the pharmaceutical manufacturers we'd appreciate it. Without objection, we'll put it in the record at this point.

Any other points anybody would like to make on this particular series of examples? Because doctors are obviously at stake in some cases, where either they're getting a kick-back or whatever. I would just be curious about what your knowledge is in that case. If they're collecting names, let's say they're in the cancer business or in the heart business, that they give those lists of names to people that have other alternatives. The question is, To what degree are they kicked-back with money on that? Any of you ever heard of that? I see seven people hear-no-evil, or something. Or is that a legitimate problem to think about?

Dr. HARDING. Something close in the National Committee on Vital and Health Statistics. The vice president of a major drug company testified that they have a record of all people who take X-medication. And I asked the question, do you ever sell that? And he said, no. I said, well, is it ever used? He said, yes, for a fee we will take information from a company, say, that wants to sell some cholesterol-lowering medicine, and we will send it to those people, but we will keep the names and so-forth within the company.

So that's using that information, not letting it out, but then marketing the people within the companies.

Mr. HORN. That's familiar to all of us who run for public office, that there are people's memberships used by mailhouses, but we'll never see them. They'll just say, gee, we did that mailing for you, Congressman. [Laughter.]

If we're curious, we always put fake names or all our relatives on to see if anything ever lands on the doorstep. But that's another business that needs something to be done to it, at some time.

Are there any questions you feel we should have been considering that we haven't considered this morning?

Yes, Dr. Korn.

Dr. KORN. Mr. Chairman, I've already made the point, I think, that the members of our association have a very global interest in these problems because they engage in education, patient care, and in research. I'd like to offer you a personal suggestion.

I understand as just a participant in this process, how difficult it is to grasp and get traction on the problem of protecting medical information as it flows through our health care delivery system. It's a large challenge to be able to get one's arms about that. I believe, and the association has so argued, that research information can, in theory, be much more tightly protected than the information that's being transmitted and used in the course of health care delivery. There is really no mandated access to research information, that I can think of, that would overcome the confidentiality of the information, if that's the standard one wishes to use.

There is a statutory provision that exists, which I think has some tremendous potential, which is called the Certificate of Confidentiality. It was adopted in 1970 in order to facilitate studies of drug-use and abuse, incompetence in veterans of the Vietnam war. And the reason that this certificate was developed was because, and I'm sure Dr. Harding knows about this very much, that people were not going to be willing to participate in these kinds of studies of

arguable criminal behavior, if they feared that their participation was going to be used to get them into trouble.

In about 1974, that certificate was introduced into the public health act at a time of reauthorization and in 1988, the provision of its protection was broadened to any biomedical, behavioral, or medical research that could develop sensitive or stigmatizing information about an individual. The way that works right now is that an investigator who is proposing a project that involves such information, applies to the Department of Health and Human Services and is granted on a project-specific basis the protections of the certificate.

There is really no reason that I can think of, and I'm not a lawyer, why that kind of protective mantle could not be imposed by Federal law over all human subjects research data that would make them almost impregnable to trespassing. In other words, that certificate will not allow anybody to get out that research data base, whether it's the employer, family, next-of-kin, law enforcement, or the legal system.

There's been one case in New York State actually, that involved a suspect in a homicide case in which the highest court in the State of New York upheld the sanctity of the certificate and prevented State authorities from getting into sensitive information. It happened to be a drug-abuse program in which the suspect was felt to be possibly lurking, and the police were unable to get into that data base, even though there was a suspicion of a major criminal offense.

The exceptions to that protection are exceedingly small. One of them is that the confidentiality protection can be violated in investigating fraud in the research. In other words, if there's a question of fraud in the research itself, people who are investigating the fraud have to be able to get in there, and see what did and did not happen. An individual subject can ask that the information be disclosed about him or herself, but otherwise it's about as impregnable a barrier to information as anything that exists in the United States.

And I see no reason in trying to deal with some of these sensitive issues, whether it's mental health, genetic information, sexually transmitted diseases, or whatever, why there could not be a provision that would put around human subjects data bases that contain these kinds of data, a very, very tight, very tight Federal protection from trespass.

That still won't prevent, excuse me, as you said, an idiot from leaking information, and there the remedy has to be severe sanctions for people who do that sort of thing, and strong behavioral codes to prevent it.

But, I do think, and again, I'm not walking away from the larger problem of the health care delivery use and information at all. But I do think that in the area of medical research there's an established remedy in U.S. law that's been used very successfully. It has never been violated in its existence.

Mr. HORN. Now, have there been other cases besides New York that have been involved with this particular certificate?

Dr. KORN. You mean in challenging a certificate?

Mr. HORN. Yes.

Dr. KORN. Not to my knowledge and I've been consulting with people at the Federal Judicial Center here in town, who are very into this kind of thing and they've told me there has never been an instance, that they know of, where someone has been able, forcibly, to get at data protected by that mechanism.

Mr. HORN. It's an interesting point because I was going to ask some further questions on research, and I think that's an important contribution to this particular area.

Are there any other questions that we should have asked that we didn't? Are you sitting there burning, saying, "why the heck can't they ask that question?" So you think we covered some of the ground?

OK.

Mrs. Maloney, any further thoughts?

Mrs. MALONEY of New York. Just, I really think that this is probably the most important issue that's come forward. It's critically important and I look forward to working with you on it.

Dr. KORN. May I, sir, may I just make one other comment? You asked a question earlier and I didn't have a chance to answer it.

Far be it for me to suggest to a Member of Congress, whether he or she should or should not draft legislation; I wouldn't presume to do that, but I would say that there's been a lot of learning in the process to date in, at least, the Bennett bill and in the Shays bill, and I think it would be just efficient in the use of your own time to take advantage of those several years of travail and benefit from the hard work that those staffs have done.

Mr. HORN. Yes, we definitely believe in economies of scale here. And the staff will be doing, with the American Law Division and the respective counsels in the Senate, a side-by-side on these to see where we are and the particular language. We want to see, based on the testimony that the seven of you have given, what's missing and what should be included. So, they will have their hands full over the next few weeks, maybe a few months.

We will get back to you because we're looking forward to getting you around the table when we see the side-by-sides. Let's go over it and spend an afternoon on it.

So with that, I thank my colleagues who showed up this morning to ask questions, and particularly, the former ranking member, we're always glad to see her back. And you probably missed another hearing as a result of your fascination.

The staff that were responsible for this hearing are staff director and chief counsel, J. Russell George. Back there against the wall, to my immediate left and your right, John Hynes is the professional staff member involved with this hearing. Welton Lloyd is a congressional fellow with us, and we're delighted to have him. Matthew Ebert, our clerk. And then, Kami White, an intern with us.

And I hear Kami, this is your last hearing? Is it? Well, we thank you for all you've done for us. We appreciate it. How many months were you here? Three? Well, you're a fast learner, Kami. So, good luck at school.

And then we have Betsy Damus, also an intern with the subcommittee.

And then for the minority, we have Karen Lightfoot, professional staff member; and Jean Gosa, clerk; and we have Margaret Hahn,

who has great patience and has been the court reporter this morning.

And we thank all of you.

And the hearing is adjourned.

[Whereupon, at 1:05 p.m., the subcommittee adjourned subject to the call of the Chair.]

[Additional information submitted for the hearing record follows:]

Consortium for Citizens with Disabilities

May 27, 1998

The Honorable Steve Horn
Chairman
House Subcommittee on Government, Management, Information,
and Technology of the Committee on Government Reform and Oversight
B-373 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

We are writing as Co-Chairs of the Health and Rights Task Forces of the Consortium for Citizens with Disabilities (CCD). CCD is a Washington-based coalition of nearly 100 national disability organizations that advocate with and on behalf of children and adults with disabilities and their families. All persons who receive health care services in this country have reason to be concerned with the inappropriate use of highly personal information that is collected about them within the health care system. As a coalition representing the 54 million people living with disabilities in the United States, however, our views on this issue are somewhat unique. We are writing to request that we be permitted to submit these comments and attachments as part of the written record of last week's hearing on medical records confidentiality legislation.

Because people with disabilities frequently need ongoing care in the treatment of their disabilities, their medical records are rather extensive and contain much highly sensitive personal information. People with disabilities are more likely to be hurt by the unauthorized disclosure of their medical records, since they are vulnerable to discrimination on the basis of their disabilities. CCD firmly believes that individuals should retain the ultimate right to decide to whom, and under what circumstances, their protected health information should be disclosed. We strongly support the passage of federal legislation that will protect the privacy and confidentiality of individually identifiable information.

Our position, however, is not absolute. We are particularly sensitive to the careful balance that must be struck when enacting legislation to protect the privacy of health information. Persons with disabilities are perhaps the primary beneficiaries of biomedical and health services research. We suffer greatly when access to efficient, quality health care is in any way hampered. We

recognize, therefore, that any privacy legislation ultimately enacted must not be so restrictive as to impede important medical research or necessary oversight and monitoring of the health care delivery system. Care must also be taken to ensure that legislation does not undermine efforts to adopt outcomes measures that will enhance quality of care.

The CCD Health and Rights Task Forces are pleased that you held last week's hearing, and that you have demonstrated a strong interest in enacting federal legislation to protect the privacy of an individual's identifiable health information. This letter outlines our positions on what we view as the "critical issues" in any medical records confidentiality legislation. We also offer an analysis of Congressman Shays' proposed legislation (H.R. 3900) in light of CCD's positions on these critical issues. We have also included CCD's Principles for Health Privacy Legislation as an attachment. We believe these principles should be incorporated in any privacy legislation.

Authorizations

The concept of informed consent means that a party who wishes to disclose an individual's health information must first obtain the individual's knowing and meaningful assent to the disclosure. Such consent creates an underpinning of trust without which our health care system could not function properly. Federal privacy legislation should require that every disclosure be subject to an authorization unless the disclosure is specifically allowed under one of the exceptions.

Individuals, generally, have concerns when the disclosure of very private information is out of their control. For people with disabilities, however, who have been historically exposed to widespread stigmatization and discrimination, unauthorized disclosure of their personal health information could result in more than just personal embarrassment -- it could also affect their ability to work, their standing in their communities, and their possible exposure to life-threatening personal violence. For this reason, people with disabilities enter any discussion of protecting health information privacy from the vantage point that they must retain control over access to their own information. Without such security, people with disabilities have powerful reasons not to access the health care system at all, whether they be people with HIV infection, people with mental illness, or people with rare and misunderstood disorders.

We understand the desire for employers and health plans to receive one authorization up front to avoid unnecessary and inefficient duplication in the authorization process. Indeed, as individuals who often interact with the health care system, we have no desire to sign multiple authorizations that are unnecessary. To address concerns that authorizations will create a burden on health care administrators' core functions, Senators Jeffords, Dodd and Bennett have proposed a two-tiered authorization structure. For authorizations that are necessary for treatment, payment, and select core functions of administration, consumers would be required to a sign an authorization at the time of enrollment into a health plan. But, for activities outside this selected core, individuals would remain free to decline authorization without fear of penalty.

We are comfortable supporting the two-tiered authorization structure because consumers will have the opportunity to be informed about how their information is going to be used, even if they don't truly "consent" to authorizations for treatment, payment, and other core operating functions. By providing such information at the beginning of the process, consumers will be more educated and less distrustful about what their identifiable health information is being used for. We are currently engaging in conversations with health care industry representatives to develop a better sense of what core functions should be included in a first-tier authorization system.

The Shays bill offers an alternative approach to the authorization process. In contrast to the Senate proposals which establish an affirmative duty to obtain an authorization for disclosures of individually identifiable information, H.R. 3900 imposes liabilities for failure to take certain actions -- including the negligent or intentional disclosure of individually identifiable health information without a valid authorization. We are pleased the bill creates a liability for unauthorized disclosures and we appreciate the effort to develop an alternative authorization structure to that proposed in the Senate. However, we find the liabilities and the exceptions included in the bill somewhat unclear. It is confusing how the requirement to obtain an authorization interacts with the exceptions. We believe it is important for the federal law to be very clear about required authorization procedures. In the absence of clarity, providers and patients will end up litigating any confusion in the courts.

H.R. 3900 also differs from the Senate proposals in the way it deals with treatment, payment, and other core operating functions. Instead of establishing a two-tiered authorization structure, the bill exempts disclosures for treatment, payment, and operating functions from the authorization process altogether. CCD understands the desire of health plans, employers, and other entities to avoid unnecessary and inefficient authorizations, but we believe it is a mistake to exempt these activities from the authorization process entirely. As a result of this total exemption, consumers would remain uninformed about who will see and use their personal medical information and the public health interest in maintaining trust between patients and their providers would be undermined. For these reasons, CCD does not support the current authorization structure in H.R. 3900. We look forward to working with Congressman Shays and his staff to address our concerns.

Research

Many people with disabilities live with conditions that are progressively debilitating, and in some cases, fatal. Others have conditions for which new therapies or new habilitation and rehabilitation techniques could significantly enhance their quality of life. People with all types of disabilities depend on research for life-saving cures or for therapeutic advancements that will make an enormous difference in the type of role they can play in society. At the same time, people with the most to benefit from the miracles of biomedical and other research are often those who are most harshly stigmatized and face the greatest obstacles of discrimination. For

this reason, CCD believes that any federal privacy legislation must strike an appropriate balance between supporting research and protecting an individual's right to privacy.

We believe that most research can be conducted without individually identifiable data. Any federal privacy legislation should create incentives to turn personal health information into nonidentifiable health information for health research -- and, for that matter, for public health, law enforcement, judicial, and administrative purposes as well. Technological means exist today for researchers and others to engage in their studies without unfettered access to individually identifiable information. Privacy legislation should create incentives for researchers to adopt new technologies that make the use of non-identifiable data the common default practice, and the use of individually identifiable data the rare exception.

While we support the disclosure of protected health information when it is absolutely needed for health research, we also believe there should be an analysis through which Institutional Review Boards (IRBs) determine whether it is reasonable or appropriate to waive the informed consent requirement based on the risk/benefits to the research project balanced against the risk/benefits to the individual whose protected health information is being disclosed. It is only by including this step of the analysis that health researchers -- both public and private -- will have an incentive to adopt new technologies that will make the use of nonidentifiable health information in research projects more prevalent.

We are encouraged that Congressman Shays shares our view that federal confidentiality protections should not impede scientific and biomedical research. We appreciate the bill's requirement that entities establish an internal review process for health research projects involving archival data. We do not believe, however, that the exception for archival research included in the proposed legislation creates the necessary incentives for researchers to use non-identifiable data whenever possible and practicable. Without some sort of external oversight of both confidentiality practices and internal review board standards, entities could allow archival research projects to use identifiable health information even if identifiable information is entirely unnecessary for the success of the project. Again, CCD proposes that the current IRB model (which is already working well for publicly funded research) should be extended to private research as well. IRBs could then weigh the interest in patient confidentiality as part of their review process.

Oversight

People with disabilities strongly support efforts to eliminate fraud and abuse in the health care delivery system. As major consumers of health care, such fraud affects us directly. We believe, however, that fraud and abuse problems can often be combated effectively by using nonidentifiable health information. While we understand that creating such incentives are difficult, CCD would like to work with staff to come up with creative approaches for achieving this goal.

In addition, we believe it is inappropriate to raid the medical records of health researchers and public health authorities unless the investigation directly involves the fraud and abuse of the researcher or the public health authority. In those limited circumstances in which a health oversight agency investigates a health researcher or a public health authority, protected health information should be given to the investigatory agency. Without a promise that protected health information will remain confidential, the public's trust in the confidentiality of health research and public health authorities will be undermined.

As with research, we are concerned that public health authorities who are exempted from the authorization requirement are not provided with incentives to use non-identifiable health information whenever possible.

Law Enforcement

We believe law enforcement officials must show "probable cause" that individually identifiable health information is necessary to the issue at hand. This standard mirrors the Fourth Amendment constitutional protections against illegal searches and seizures.

We support the bill's acknowledgment that there should be some assessment of whether the need for identifiable medical information outweighs the privacy interest of each individual. However, the balancing process offered in the bill is not as strong a privacy protection as the constitutional standard for searches and seizures. The traditional "probable cause" standard should be the statutory standard as well and the balancing process currently included in the bill should be used to supplement this protection. Also, we understand there are some laws requiring health care providers and others to disclose certain types of medical information to law enforcement officials (i.e. gun shot wound reporting). However, we believe the bill's terms create too broad an exception for such disclosures. The bill allows disclosures for any "request[s] otherwise authorized by law from a law enforcement agency." We believe the laws at issue, such as gun shot wound reporting, should be specifically listed in the legislation. Otherwise, this exception creates a possible loophole for a range of unauthorized disclosures.

Preemption

We believe federal privacy legislation should ensure a basic level of protection for everyone. If states, however, through statutory or common law, decide to provide greater privacy protections, we believe those initiatives should be honored. Such an approach is consistent with other federal civil rights law.

In any event, we believe that state laws governing the confidentiality of mental health information and communicable disease statutes should be excluded from the pre-emption provisions. State law carefully weighs public health concerns against the complex issues of

discrimination and stigma facing people with mental illness, people living with HIV/AIDS, and others. Federal privacy law should not preempt the carefully tailored state laws in these areas.

Although CCD continues to advocate against federal preemption, we strongly support H.R. 3900's carve outs for mental health and communicable disease laws. We appreciate the acknowledgment that state laws in these areas are often complicated and represent a careful balance between public health concerns and personal privacy.

We look forward to working with you and your staff on medical records confidentiality legislation. In addition to the remarks in this letter, we have various other concerns we will be communicating to you in the near future.

If you have any questions about any of these comments or would like CCD's assistance, you may contact CCD through Jeff Crowley at the National Association of People with AIDS (202-898-0414).

Sincerely,

Health Task Co-Chair

Jeffrey Crowley
National Association
of People with AIDS

Rights Task Force Co-Chair

Curt Decker
National Association of
Protection and Advocacy Systems

Prepared by the Georgetown Federal Legislation Clinic on behalf of NAPAS/CCD. (h:\katie\ccd\privacy\shays.526.5.27.98)

Consortium for Citizens with Disabilities

PRINCIPLES FOR HEALTH INFORMATION PRIVACY LEGISLATION

The Consortium for Citizens with Disabilities (CCD) is a coalition of approximately 100 national consumer, advocacy, provider and professional organizations that advocate on behalf of the over 49 million persons with disabilities in the United States. CCD works on a range of issues -- from health care and education to civil rights and housing. As advocates for persons with disabilities, CCD strongly supports the passage of federal legislation that would protect the privacy and confidentiality of individually identifiable health information -- particularly, legislation that requires meaningful notice and informed consent prior to the waiver of a person's privacy rights. CCD believes, however, that any such legislation must also protect the continued viability of medical research and the continued delivery of quality health care. Toward that end, CCD adopts the following principles:

Federal legislation should statutorily establish an individual's right to privacy with respect to individually identifiable health information, including genetic information. Individuals should retain the ultimate right to decide to whom, and under what circumstances, their individually identifiable health information will be disclosed. Confidentiality protections should extend not only to medical records, but also to all other individually identifiable health information, including genetic test results, clinical research records, mental health therapy notes, etc.

Federal legislation should prohibit the use or disclosure of individually identifiable health information absent an individual's informed consent. Health care providers, insurance companies, and others in possession of individually identifiable health information should be prohibited from using or disclosing such information unless authorized by the individual. In addition, any information used or disclosed should be limited to the minimum amount necessary for the use or disclosure. Unauthorized disclosures should be permitted only under exceptional circumstances -- for example, if a person's life is endangered, if there is a threat to the public health, or if there is a compelling law enforcement need.

Federal legislation should guarantee an individual the right to access his or her own health information and the right to amend such information. Individuals should have the right to access and amend their own medical records so that they can make informed health care decisions and can correct erroneous information in their records.

Federal legislation should establish strong and effective remedies for violations of privacy protections. Remedies should include a private right of action, as well as civil penalties and criminal sanctions where appropriate.

Federal legislation should provide a floor for the protection of individual privacy rights, not a ceiling. Like all other federal civil rights and privacy laws, federal privacy legislation for health information should set the minimum acceptable standard. Federal legislation should not pre-empt any other federal

or state law or regulation that is more protective of an individual's right to privacy of or access to individually identifiable health information.

While protecting individual privacy rights, federal legislation should not impede important clinical and medical research. Federal privacy protections should not hinder the conduct of biomedical research and development. For example, researchers should be allowed to continue using existing anonymized patient databases and tissue samples. We believe, however, that "research" should not be defined so broadly as to permit the disclosure of individually identifiable health information for marketing or commercial purposes.

Endorsing Organizations (List in formation)

AIDS Action Council
The Arc
American Association on Mental Retardation
American Counseling Association
American Network of Community Options and Resources
American Speech-Language Hearing Association
Americans with Disabilities Vote
Bazelon Center for Mental Health Law
BETHPHAGE
Children and Adults with Attention Deficit Disorders
Council for Exceptional Children
Epilepsy Foundation
Human Rights Campaign
Justice for All
Legal Action Center
National Alliance for the Mentally Ill
National Association of Developmental Disabilities Councils
National Association of People with AIDS
National Association of Protection and Advocacy Systems
National Association of Social Workers
National Council for Community Behavioral Healthcare
National Easter Seal Society
National Multiple Sclerosis Society
National Organization on Disability
National Organization for Rare Disorders
Paralyzed Veterans of America
RESNA Rehabilitation and Assistive Technology Society of North America
Spina Bifida Association of America
Star Program
Unitarian Universalist Association of Congregations
United Cerebral Palsy Associations

For more information, contact Jeff Crowley, NAPWA at 202-898-0414.

Prepared by the Georgetown Federal Legislation Clinic on behalf of NAPAS/CCD (h:napascd/spring.98/lester/principl.wpd)

I. Introduction

The American Association of Health Plans (AAHP) is the largest national organization of health plans. AAHP represents more than 1,000 health maintenance organizations (HMOs), preferred provider organizations (PPOs), and similar network-based plans. Together, AAHP member plans provide quality health services for approximately 140 million Americans. AAHP member plans are dedicated to a philosophy of care that puts patients first by providing coordinated, comprehensive health care.

The subject of today's hearing -- how to craft federal legislation to protect against inappropriate use of patient-identifiable health information, while at the same time permitting the coordination and delivery of high quality health care -- is one of the most important issues facing federal health policy makers today. Not only is there great potential for harm if patient information is misused, but our health care system relies on patient trust as an essential ingredient to quality health care. The use of patient information by health care providers, health plans, and health researchers has already greatly improved the quality of health care. Continued use of this information will enable us to build on that improvement.

This statement highlights how health plans currently use patient-identifiable health information to support quality assurance and improvement programs and emphasizes the importance of properly structuring federal confidentiality legislation in order both to preserve patient confidentiality and ensure that quality of patient care can continue to be enhanced.

II. Health Plans Support Safeguarding the Confidentiality of Patient-Identifiable Health Information

AAHP and its member plans strongly support the goal of assuring consumers that health plans and health care providers will respect the confidentiality of their identifiable health information. We believe that appropriate confidentiality safeguards for patient-identifiable information are essential to ensuring that health plan members feel comfortable communicating honestly and openly with their physicians and other providers. Without open communication between patients and their providers, treatment decisions are based on incomplete or inaccurate information and quality of patient care suffers.

AAHP's member plans have demonstrated their commitment to confidentiality by addressing this issue as part of AAHP's ongoing *Putting Patients First* initiative. Because AAHP is committed to addressing the issue of consumer confidence in health plans, association members must meet standards related to confidentiality. Member plans must safeguard the confidentiality of patient-identifiable health information through policies and procedures that, consistent with federal and state law, (a) address safeguards to protect the confidentiality of patient-identifiable health information; (b) provide for appropriate training of plan staff with access to patient-identifiable information; and (c) identify mechanisms, including a clear disciplinary policy, to address the improper use of patient-identifiable health information. The policy reinforces that health plans should not disclose patient-identifiable health information without the patient's consent, except when necessary to provide care, perform essential plan functions such as quality assurance, conduct bona fide research, comply with law or court order, or for public health purposes.

This policy on confidentiality joins other policies that are also part of AAHP's *Putting Patients First* initiative, covering areas such as information for consumers, physician-patient communication, choice of physician, grievance and appeals, physicians' role in plan practices, and, of course, quality assessment and improvement.

Virtually all of the current federal legislative proposals related to confidentiality recognize that health plans need access to patient-identifiable information for purposes of facilitating treatment and securing payment for health services. However, one area where there continues to be some confusion over health plans' need for information relates to health plans' efforts to improve quality of care.

It is true that, for some of the quality-enhancing activities health plans undertake, they are able to use non-identifiable health information -- information that has been aggregated, anonymized, coded, or encrypted in such a way that the information no longer reveals the identity of particular individuals. Consistent with the vast majority of legislative confidentiality proposals that have been considered to date, AAHP believes that a patient's interest in confidentiality is pertinent only when his or her *identifiable* information is involved. Because aggregate, anonymized, coded, or encrypted information does not identify individuals, consumers need not be concerned about the use of this information.

However, some of the fundamental, quality-enhancing activities undertaken by health plans *do* require the use of identifiable health information. The use of health information in health plan

quality assurance and improvement activities can greatly enhance the quality of health care for both the individual plan member and the member population as a whole, and AAHP believes that health plan members should benefit from these quality improvement activities. These activities are not only fundamental to coordinated, quality care, but in many cases are also required of health plans under a variety of state and federal programs and regulations, as well as under voluntary private sector reporting and accreditation standards.

III. Health Plans Use Patient-Identifiable Health Information to Enhance Quality

Health plans use patient-identifiable health information in a variety of activities that improve the quality of health care. These activities, which focus on both the processes of delivering care as well as on the outcomes of care, include health promotion and prevention, disease management, outcomes research, and utilization management. Health plans' ability to enhance quality through these activities could be seriously jeopardized unless federal confidentiality legislation is properly structured.

Health Promotion and Prevention

Health promotion and prevention activities improve quality by enabling plans and providers to identify members at risk for certain illnesses or eligible for certain services. Plans and providers can then reach out to those members to provide information to them and encourage them to seek out services when they can benefit most from intervention and before disease progresses. Often, determining who is at risk involves the use of patient-identifiable health information. Health plans add much of value in this area because they have access to claims data and can help busy

physicians accurately identify patients at risk of certain illnesses or who are eligible for certain services -- even among patients the physician may not have seen in some time. Once the plans have identified these members, they contact them and, in many cases, the members' physicians as well. Many plans encourage their physicians to follow-up with the identified members to schedule the necessary appointments.

For example, nearly all plans have implemented postcard or phone-call mammography reminder systems for their female members. Patient-identifiable information is used to identify female enrollees of a certain age who have not received a recent mammogram. United HealthCare's plans use patient-identifiable information to single out women aged 50 to 74 who are overdue for a mammogram. The plans send reminder notices to these women as well as to their physicians so that the physicians can follow-up with their patients directly. As a result of this program, in 1995, United HealthCare's plans across the country experienced increases in mammography rates ranging from 30-45%. This program and others like it promote detection of breast cancer in the earliest and most treatable stages.

Disease Management

Disease management activities improve quality by identifying members who have been diagnosed with certain chronic diseases and then coordinating and monitoring their care. Again, because health plans have access to claims data, they are well-positioned to identify those members who will benefit most from disease management programs. Health plans then contact the identified members and, in many cases the members' physicians, in order to encourage them to seek the

appropriate care.

For example, according to a recent study, 45.4% of all HMOs had diabetes disease management initiatives in place in January 1996.[1] Harvard Pilgrim New England has developed a comprehensive gestational diabetes management program that includes directed case management and regular vision screenings. The plan uses patient-identifiable information to identify members with diabetes and involve them in the plan's disease management program. As a result, the plan was able to increase annual retinal exams by 26%, eliminate diabetes-related newborn major malformations, and decrease the incidence of low blood sugar reactions in patients receiving insulin therapy.

Asthma management is another area where health plans use patient-identifiable information to target members and improve the quality of care delivered to them. As of January 1996, 50.4% of all HMOs had asthma management programs in place.[2] PrimeCare Health Plan, for example, examines clinic and hospital record information to identify children with asthma who are missing an inordinate number of clinic appointments and who have high hospital admission rates. Working with the children's pediatricians, the plan involves the children and their families in an asthma education and management program that initially resulted in a 30% reduction in emergency room visits and a 60% reduction in hospital admissions for participants of the program.

---

[1]The InterStudy Competitive Edge Part II: Industry Report, September 1996, p. 76.

[2]Ibid.

Outcomes Research

Another method health plans use to improve the quality of care is outcomes research. Health plans use patient information to evaluate the effect of particular treatment programs, assess the typical course of a chronic disease over time, and identify variations in outcomes that may be targeted for future improvements in health care processes.

For example, Kaiser Permanente of Northern California used patient-identifiable information to study the most effective treatment for a type of diabetes. Using identifiable health information of their members who had been treated for diabetes, Kaiser studied whether patients who matched a certain clinical profile and were treated with the drug Metformin experienced better outcomes than patients who did not have the same profile but who were also treated with Metformin. The outcomes analysis indicated that, in fact, outcomes were better in the patients who matched the profile than in those who did not match the profile. This study provided Kaiser physicians with the clinical evidence needed to select the most effective course of therapy for their diabetic patients.

Utilization Management

Utilization management activities involve evaluating the medical necessity and appropriateness of health care services both for the purposes of payment as well as for quality improvement. Utilization management enables plans to respond to inappropriate patterns of care. For example, evidence suggests that hysterectomies and caesarean section deliveries are over-performed in the U.S. Hysterectomies are the second most common procedure -- performed on 1 in 3 American

women by the age of 60. In Italy, by comparison, the figure is 1 in 6 and in France it is only 1 in 18. Similarly, the Centers for Disease Control estimated that physicians performed 349,000 unnecessary caesarean section deliveries (approximately 1 out of every 12 deliveries) in 1991 -- unnecessarily placing women at risk of infection and unnecessarily exposing them to the complications and trauma associated with major abdominal surgery. Health plans' utilization management programs require patient-identifiable information to ensure that patients receive necessary, appropriate, high-quality care in a cost-effective manner.

Integrated Delivery of Services

Integrated delivery of services enables health plans and providers to utilize patient-identifiable health information in even more ways to improve the quality of care. Often, physicians are provided with increased access to patient information in order to aid them in their management of certain health conditions. For example, physicians at LDS Hospital in Salt Lake City created a computer-assisted management program for antibiotics and other anti-infective agents which Intermountain Health Care now uses in its hospital intensive care settings. The program compares historical patient data (rendered non-patient-identifiable) on infection characteristics and antibiotics effectively used in treatment to current patient infection data. The system then provides decision support to physicians by recommending anti-infective regimens and courses of therapy based on its comparison. The system also helps to prevent adverse drug reactions and promote cost-effective care by enabling physicians to choose anti-infective regimens that are the most

effective for the lowest cost.[3] In this example, patient-identifiable information that has been rendered non-identifiable is used to link previous patient record information on infection causes and treatment regimens to the computer-assisted antibiotic management program to improve care for current patients.

As previously mentioned, not only are these activities that use patient-identifiable information fundamental to improving patient care, but many are also required of health plans under a variety of state and federal programs and regulations, as well as under voluntary private-sector reporting and accreditation standards. For example:

* Activities to monitor, detect, and respond to over- and under-utilization are required by state HMO and utilization review laws, federal laws, and private accreditation standards;

* Data collection and analysis of condition-specific patient outcomes are required of plans participating in the Federal Employees Health Benefits Program;

* Ongoing quality assurance programs that (1) stress health outcomes and provide for the collection, analysis, and reporting of data; (2) monitor and evaluate high volume and high risk services and the care of acute and chronic conditions; and (3) after identifying areas for improvement, take action to improve quality, are required of Medicare+Choice plans under Medicare;

---

[3] Evans RS, Pestotnik SL, Classen DC, et. al., "A computer-assisted management program for antibiotics and other antiinfective agents," New England Journal of Medicine, January 22, 1998; 338:232-8.

* Procedures to ensure health care delivery under reasonable quality standards, consistent with recognized medical practice standards, and ongoing, focused activities to evaluate health care services, are required by the NAIC Model HMO Act, which approximately 30 states have adopted;

* Quality management programs that "monitor, evaluate, and work to improve the quality of care and quality of services provided . . . utilizing a variety of quality management studies, reviews, and evaluations such as . . . medical record reviews" are required of plans seeking URAC/AAHCC accreditation;

* Quality management standards that monitor aspects of patient care such as disease management, acute and chronic care, and preventive care are also required of plans seeking URAC/AAHCC accreditation;

* Health management systems that identify members with chronic conditions and offer appropriate services and programs to assist in managing their conditions are required of plans seeking NCQA accreditation; and

* Actions and interventions to improve quality by addressing opportunities for improved performance are also required of plans seeking NCQA accreditation.

It is clear that health plans' efforts to improve patient care have been recognized by state, federal, and private regulatory entities alike. It also should be clear that compromising plans' abilities to improve patient care -- whether by imposing excessive regulatory requirements or by leaving plans with inadequate or partial information for quality studies -- would result in reduced quality of care. This would present an obvious quandary for plans legally and contractually required to conduct quality-enhancement activities, yet at the same time forbidden to use the information necessary to

fulfill these obligations.

IV. Unduly Restricting Health Plan Use of Patient-Identifiable Health Information Would Reduce Quality

Some of the current federal confidentiality proposals include provisions which would unduly restrict health plan use of patient-identifiable health information and, as a result, seriously threaten quality of care. One of the more restrictive and quality-compromising approaches put forth would be to require health plans and providers to obtain patient authorization each and every time they use identifiable health information. This type of authorization requirement would be impractical, costly, and a major burden for patients as well as for plans. Moreover, the nature of many of these plan activities is that they are *seeking to identify* individuals at risk -- it would be impossible to obtain consent from individuals who had not yet been identified. As a result, health plans would be unable to send mammography reminder notices or information on asthma management programs to plan members in need of these services.

A second approach to restricting the use of patient-identifiable information for quality-enhancing purposes which has also been proposed by some would be to permit patients to opt-out of participating in quality-enhancing activities, such as health promotion, disease management, outcomes research, and utilization management. Such an opt-out provision would diminish the capacity of current health plan quality assurance programs and be counterproductive to improving the quality of patient care. In fact, withholding some patients' information within a health plan setting could make engaging in these quality-enhancing activities so impractical that plans and

providers would forgo these activities for *all* patients -- again, raising the potential conflict between plan obligations to improve quality and legal restrictions on the use of the information needed to fulfill those obligations. For example, in the case of the computer-assisted management program for antibiotics, if patients were permitted to object to the use of their medical record information for this program, the data available to physicians would be incomplete and could skew the computer-generated treatment recommendations, potentially threatening the quality of care not just for the patient who opts out. but for *all* current patients. Such a threat could likely prompt the discontinuation of this innovative and much-lauded program. This would also be true for other quality-enhancement endeavors of this type.

Leaving plans with incomplete information could also force current state, federal, and private reporting and quality improvement requirements to be modified and weakened to reflect the health plans' diminished capacity even to report on health outcomes or enrollees' use of services. This in and of itself would make plan quality improvement less effective and accreditation status less meaningful. On a more global level, our national goal of finding out the most effective ways to deliver health care -- to make sure that patients get the best care for their health dollar -- would be severely compromised.

V. A Statutory Authorization Would Preserve Quality of Care With Fewer Procedural Barriers

For the reasons just mentioned in the previous section, AAHP supports the inclusion of a statutory authorization in federal confidentiality legislation. A statutory authorization would authorize in

law all of the widely accepted positive uses of patient-identifiable health information, including facilitating treatment, securing payment, and conducting health plan quality-enhancing activities. Both the Administration's proposal and the National Association of Insurance Commissioners' (NAIC) draft Health Information Privacy Model Act follow the statutory authorization approach. A statutory authorization would achieve the goal of providing plans and providers with access to identifiable health information to improve quality of care. And, by working in tandem with strong penalties for the *misuse* of identifiable health information, a statutory authorization would also achieve the goal of assuring consumers that plans and providers will respect the confidentiality of their identifiable health information. It is AAHP's recommendation that any penalties be consistent with the penalties already established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for the wrongful disclosure of individually identifiable health information.

A slightly less effective alternative to the statutory authorization that has also been proposed is the consolidated authorization. As proposed, the consolidated authorization would allow plans to procure a single authorization at the time of enrollment to use identifiable health information for the purposes of facilitating treatment, securing payment, and conducting quality improvement activities central to patient care. While the consolidated authorization is a vast improvement over having to obtain separate authorizations each and every time patient-identifiable information is used, this approach has limitations that the statutory authorization does not.

For example, one legislative proposal that has followed the consolidated authorization approach has also included provisions permitting revocation of that consolidated authorization. Yet, expecting health plans to facilitate and pay for quality health care services after a patient has revoked his or her prior authorization for use of health information is a Catch-22 for health plans. Not being able to use patient-identifiable information would interfere with plans' abilities to effectuate payment for services already rendered, facilitate and coordinate treatment, and fulfill legally required operational functions -- in essence, paralyzing plans' ability to effectively serve patients. On the other hand, plans -- and physicians and hospitals -- could be held criminally liable for continuing to facilitate high quality treatment by using identifiable information.

This particular legislative proposal has addressed this dilemma by giving health plans explicit permission to disenroll individuals from the plan upon the individual's revocation of his or her authorization. While health plans prefer not to have to disenroll patients, revocation provisions often provide them no choice. In fact, given the liability involved for unauthorized use of information as well as for substandard care, revocation by an enrolled individual should perhaps be treated as disenrollment without requiring any further action by the plan. It should also be noted that plans may have underway at the time of an individual's revocation quality improvement activities, such as outcomes research, that would continue to require the use of the patient's identifiable health information lest the entire endeavor be compromised by an individual's withdrawal of his or her information mid-study. This again points to the superiority of the statutory authorization approach.

VI. The Same Level of Protection Should Be Required for All Types of Patient-Identifiable Health Information

AAHP believes that federal confidentiality legislation should require the same level of protection for all types of patient-identifiable health information. Health care providers rely on the completeness of medical records in their treatment of patients. Segregating certain types of health information, such as genetic information, from the rest of the medical record could interfere with a provider's access to health information that can just as easily be a predictor of future health problems as other types of health information. Because of this, current practice in most health plans supports uniform treatment of all health information and, in many cases, genetic information is an integral part of the medical record indistinguishable from other personal health information. For example, given a notation of a positive marker for one of the breast cancer genes in a patient's record, a physician can encourage increased mammography screenings to detect any breast cancer tumors at an earlier and more treatable stage.

Moreover, oftentimes genetic information may not be any more sensitive than other medical record information. HIV status, treatment for mental health, reproductive history, or evidence of sexually transmitted disease can be considered equally sensitive information. Because many types of health information can be considered sensitive, singling out information based on its *presumed* sensitivity would only promote inconsistent protections.

With advanced software capabilities available, it is far preferable to limit access to information through the use of passwords and other software controls than to require plans and providers to

physically store different types of information separately or treat different types of information differently.

VII. There Should Be Nationally Consistent Rules in Areas that Affect Computerized Information Systems

AAHP believes that, given the complex and interstate nature of the way information flows in today's health care system, federal confidentiality legislation should address the need for nationally consistent rules in areas that affect computerized information systems. Moreover, consistent rules governing disclosure of various portions of computerized health records will facilitate compliance by multi-state health plans and employers.

VIII. Patients Should Have the Opportunity to Inspect, Copy, and Request Amendment To Their Identifiable Health Information

AAHP supports patients having the opportunity to inspect, copy, and request amendment to their identifiable health information. Federal confidentiality legislation should recognize, however, that health plans that arrange for services through provider networks typically do not maintain central medical records files. While health plans that employ salaried physicians and those that contract with physician groups whose practice is solely focused on serving the health plan's members may be prepared to provide their members with access to a comprehensive medical record, even members of these plans may occasionally seek care outside of the plan's affiliated providers. Given that it is a provider who originates health information, we believe it is appropriate for providers to be responsible for facilitating access to records and appropriate amendment

procedures. Federal legislation should permit health plans to direct patients wishing to inspect, copy, or request an amendment to their record, to their physician or other provider who originated the information in question.

In addition, some proposed legislation includes a requirement to include patients' written requests for amendments and written statements of disagreement in the patient's medical record. However, for the growing numbers of plans and providers that utilize electronic medical records, this requirement would entail transforming the patient's written statements into electronic format in order for it to become part of the medical record. Instead, AAHP suggests that a notation concerning the patient's request to amend or statement of disagreement fulfill any such requirement.

IX. Research

Any provisions targeted to research in federal confidentiality legislation must ensure that intra-plan quality improvement and other health plan operational activities are not suddenly subject to a federal oversight process that was intended for the protection of human subjects participating in clinical research and that was never intended to encompass routine quality improvement activities related to health care treatment and payment. Intra-plan quality improvement activities should not be subject to federal oversight.

Federal confidentiality legislation must also ensure that those health plans and providers that wish to provide patients access to clinical trials may continue to do so without being subject to a federal

research approval process. Current federal oversight of clinical trials already subjects researchers to review by an independent board specially designed to protect and safeguard the interests of human subjects.

X. Conclusion

AAHP wholeheartedly supports the goal of assuring consumers that health plans and health care providers will respect the confidentiality of their identifiable health information. At the same time, AAHP believes that consumers should benefit from the quality-enhancing activities health plans undertake -- many of which are required by public regulators and private sector oversight entities. In order to craft federal confidentiality legislation that achieves these two goals, it is essential to have a firm understanding of how our current health care system works, how information flows within the system to make it work, and how health plans use information to improve the quality of health care.

In this statement, AAHP has highlighted the following recommendations for federal confidentiality legislation:

> (1) Federal confidentiality legislation should not unduly restrict health plan use of patient-identifiable health information. Instead, legislation should statutorily authorize the use of patient-identifiable health information for the purposes of facilitating treatment, securing payment, and conducting health plan quality improvement activities central to patient care. This statutory authorization would work in tandem with penalties for misuse that are consistent with HIPAA.

(2) Federal confidentiality legislation should require the same level of protection for all types of patient-identifiable health information.

(3) Federal confidentiality legislation should address the need for nationally consistent rules in areas that affect computerized information systems.

(4) Federal confidentiality legislation should permit health plans to direct patients wishing to inspect, copy, or request an amendment to their record, to their provider. In addition, any requirements to include written statements submitted by the patient in the patient's record should permit plans and providers to include a notation of that a written statement exists if it is more technologically feasible to do so.

(5) Any research provisions included in federal confidentiality legislation must be carefully constructed to ensure that intra-plan quality improvement activities are not suddenly subject to a process that was intended for the protection of human subjects participating in clinical research and that was never intended to encompass routine quality improvement activities related to health care treatment and payment. In addition, any research provisions must ensure that those health plans and providers that wish to provide patients access to clinical trials may continue to do so without being subject to a federal research approval process. Current federal oversight of clinical trials already subjects researchers to review by an independent board specially designed to protect and safeguard the interests of human subjects.

We look forward to working with the Committee in its continued work on federal confidentiality legislation.

Good morning, my name is Joanne Denise. I am an insurance agent from Nashville, Tennessee. I am here today representing the National Association of Health Underwriters. NAHU's 15,000 members are health insurance professionals involved in the sale and service of group and individual health insurance and related products. We appreciate this opportunity to express our views on genetic information and its relationship to access to health insurance and confidentiality.

The Health Insurance Portability and Accountability Act of 1996 states that group health insurers cannot deny or take into account genetic information in the group underwriting process, unless that genetic information has already resulted in a diagnosis of illness. HIPAA does not address the issue of genetic information in the individual underwriting process. HIPAA also requires that Congress pass legislation by August 1, 1999 on confidentiality of all medical records.

Since the enactment of HIPAA we have seen a number of new bills filed relating to discrimination based on genetic information in the underwriting and employment process. The problem is, no two bills have the same definition of genetic information! A few bills define genetic information as the results of tests on DNA, RNA, and related gene testing. Others call for a definition of genetic information which would include not only information obtained via DNA, RNA, and related gene testing, but would go so far as to include personal and family medical history, and possibly the results of other lab work as well.

Why should we care what definition is used? Fortunately, in my state, individual health insurance policies are still medically underwritten. That means if someone can't pass the medical questions on a health insurance application, they can be turned down for the policy they are applying for. Medical questions on individual health insurance policies are usually similar from one insurance carrier to another. They ask about illnesses a person has had over the past five years, smoking status, current medications, and sometimes, family medical history. We have conducted a survey of members across the United States, and have not discovered any insurance companies who asked questions about genetic testing on an application for health insurance. When the insurance company evaluates the individual's application for insurance, they usually use a point system. Each medical component on the application will be worth a certain number of points. So, if a person has a pretty clean bill of health but family medical history showed that one parent died of a stroke at age 55, this would not preclude someone from being issued a policy. It might be worth 5 points out of a possible 25. But if that same person were overweight, smoked, and had unstable high blood pressure PLUS a parent who had a stroke at age 55, that family history would be a very important component of overall risk assessment. It would still be worth only 5 points, but when combined with the other risk factors, might be a factor in a person being turned down for an individual health insurance policy. Depending on what state a person lives in, someone who has been turned down for individual coverage can usually apply for coverage through a state high risk pool, or through some other state program such as the one we have in Tennessee

called TennCare. The majority of people, from our estimates, probably 70-80 percent, qualify for coverage under an individual policy based on the information provided on their application, at a reasonable rate. Medical underwriting keeps the rate down, which is extremely important in the individual health insurance market, because people who buy in the individual market don't have an employer subsidizing their premiums. That is why it is so important that we keep premiums as low as possible for as many people as possible in order allow more people to be insured.

Why is underwriting necessary in the individual market? When an **employer** buys coverage for his or her employees, that employer is subject to group insurance purchasing laws in their state. These laws provide for specific eligibility requirements which regulate when individuals may enter plans and provide for employer contributions toward health plan premiums. The combination of employer contribution and rules about when someone may enter a plan ensure that a large enough number of individuals participate in the plan and that there is little chance of one individual coming on to a plan only when they have already developed an illness. This enables plans to spread risk associated with the plan over a larger number of persons. Larger numbers of persons over which risk may be spread result in the need for less medical underwriting for the group.

Individuals buying health insurance have no rules as to when they are allowed to apply for coverage. And, as we said before, they have no employer contribution towards the cost of their coverage. So, while we hope people would be wise enough to know they

should have coverage, the fact is that they may have some other reason to think they need coverage, in the individual market. Because of this, individual policies are medically underwritten in most states to avoid what we call adverse selection. Adverse selection occurs when the normal rules of risk assumption used by insurance companies are disrupted by someone manipulating the process for their own benefit. Adverse selection causes claims payments to be higher than normal, and this results in premium increases to all policyholders. There is some speculation about what level of premium increase will cause someone to drop coverage, but it is clear that the first people to drop coverage will be those people who perceive a lesser need for the coverage - in other words, those that are healthy. Removing the healthy individuals from the pool makes the ratio of premiums to claims spiral even higher, causing rates to rise even more, resulting in an even greater number of uninsured individuals.

In states where individual health insurance policies are guaranteed issue with no health questions, premiums have increased dramatically, and carriers have exited the market. This has resulted in an extremely limited number of choices for individual health insurance consumers.

This is where the question of definitions relative to genetic information come into play. Taking away the ability ask applicants about personal and family medical history is tantamount to taking away the health questions altogether. **This is the same as guaranteed issue**. Guaranteeing to issue health insurance coverage in the individual

market where there is not an adequate mechanism to spread risk will increase the cost. And this is the market most sensitive to those increases, again, because health insurance consumers purchasing individual policies do not have employers subsidizing the cost of their health plans.

NAHU supports the prohibition of the use of genetic information in the underwriting process **PROVIDED** that the definition of genetic information is limited to DNA, RNA, and related gene testing. We believe that at this time, a genetic marker for illness cannot necessarily be considered a credible part of risk assessment on an individual or group. Expanding the definition to include personal and family medical history, however, will interfere with normal individual health insurance policy underwriting and will result in higher premiums to the consumer. The result of these higher premiums will be greater numbers of uninsured individuals. Access to a health policy which is too expensive to afford is not really access at all.

On the issue of confidentiality as it relates to genetic information, we recognize that some groups have called for specialized confidentiality standards on certain "specially protected" portions of a person's medical records, such as information on genetic testing, mental health history, or HIV status. NAHU is opposed to this separation of records for two reasons.

First, this approach forces attention away from the importance of protecting the entire medical record. While we are focusing on genetic privacy today, it is important to note that different individuals have differing ideas about which parts of their medical records are most sensitive. One person may be most sensitive about the results of a genetic test, while another may be concerned about a record of cosmetic surgery. It is impossible for us to know what each person would choose to keep in a "super secret" file, if they had the choice.

Our second concern relates to the practical aspect of keeping two sets of files. In my office, for example, I retain copies of applications for individuals as well as employer groups which apply for coverage. On small employer plans, individual employees also complete medical questionnaires. So I may actually have these records on each of 50 employees for each of the 100 employer groups we service, plus all of the individuals who apply for coverage. Depending on what Congress decided would be kept in which file, not only would I have to duplicate each file, but I would have to rescreen each application and block out information which could not be retained in the standard file. I work in an insurance agency, which handles the initial paperwork on an insurance application. Insurance companies would have to do the same thing. Doctors would have to complete two different medical records, and shift back and forth between both records. All other providers would be required to do the same thing. Not only would the chance for errors in the delivery of medical care increase dramatically, it would greatly increase

the cost of delivery of health care. For these reasons, NAHU cannot support a confidentiality proposal which calls for dual recordkeeping and disclosure requirements.

Thirty four states currently have some form of confidentiality standards which have been enacted at the state level. Secretary Shalala and some others have suggested that new federal standards should be a "floor", allowing the states to adopt more stringent standards. Many others believe that the interstate way medical care is delivered in today's society, the cost implications of fifty separate sets of standards, and the potential confusion for providers and payers, especially those which operate on or near state lines, call for a uniform system nationwide. NAHU believes that a uniform national system would be more easily understood by patients, providers, and payers, and that a single uniform system would be more cost effective.

We thank you for this opportunity to testify and welcome any questions you may have.

Testimony of the American Association of Occupational Health Nurses (AAOHN)

before the United States House of Representatives,

Committee on Government Reform and Oversight

Subcommittee on Government Management, Information and Technology

on Health Care Information Privacy and Confidentiality

May 19, 1998

The American Association of Occupational Health Nurses, Inc. (AAOHN) appreciates the opportunity to submit written testimony to the House Committee Government Reform and Oversight, Subcommittee on Government Management, Information and Technology for the hearing record on the matter of Health Care Information Privacy and Confidentiality. We want to thank the Chairman Horn and express our special appreciation for his leadership on this important issue.

Our primary interest in participating in these hearings is to urge Congress, in the strongest terms, to enact truly comprehensive medical records confidentiality legislation. In summary, we believe that for Congress to be successful in this area, it must craft legislation that will ensure that all medical records are protected under the law regardless of the mode of payment or the setting where the health information is obtained or maintained.

AAOHN is the professional association for more than 13,000 occupational and environmental health nurses who provide on-the-job health care for the nation's workers. Occupational health

nurses are the largest group of health care providers at the worksite. As such, our professional nurses assume responsibility for all aspects of health and safety for individual workers and the work environment. AAOHN supports the development of uniform laws, rules and procedures governing the use and disclosure of health care information. AAOHN has had a long-standing interest in the confidentiality of health information debate. We have developed our position statements and guidelines to ensure that the voice of the occupational and environmental health nurse is heard in Washington.

BACKGROUND

In the course of their jobs, occupational health professionals collect a great deal of personal information about the health and lifestyles of their company's employees. AAOHN members are responsible for a great deal of data collection and maintenance of personal health information. This often includes records that document medical and/or health surveillance activities, wellness programs, pre-job placement and return-to-work physical examinations, and other similar types of worksite health initiatives. It is our observation that, to date, the confidentiality issues surrounding the protection of health information gathered and maintained at the worksite have gone largely unnoticed in the confidentiality debate. Health care information obtained and maintained at the worksite is both personal and sensitive. Clearly, health information records found at the worksite are as important to the confidentiality interests of the nation's workers as the patient data contained in the more traditionally thought of

medical record. This information, if improperly used or released, may be as equally harmful to an employee's interests as any other.

AAOHN maintains that employers should have access only to that amount of health information necessary to determine whether a worker may perform his or her job in a safe manner. For example, we believe that in cases of fitness for work exams (e.g., medical surveillance records, employee assistance programs, health screening, return-to-work physical records) health care professionals should provide the employer with a written determination based on the medical record rather than handing the employer the actual record itself.

Also, in cases in which workers' compensation benefits are at issue, information obtained through the company's wellness program should not be used to defeat the claim. Employees seeking medical or disability payments under state workers' compensation laws should not be forced to sign releases covering their entire medical record in order to file their claim. Only information directly relevant to the illness or injury underlying the compensation claim and any appropriate secondary injury determination should be available. No other information should be released without meaningful, uncoerced consent on the employee's part for a more expansive disclosure.

Limiting the amount of personal health information an employer may learn about his or her employee is not a novel or untested regulatory approach. The "bloodborne pathogens"

regulations issued by the Occupational Safety and Health Administration (OSHA) explicitly requires that such information must be kept confidential and "not disclosed or reported without the employee's express written consent to any person within or outside the workplace except when required by this section or as may be required by law."[1] The law also narrows the extent of the information provided to the employer to that which is necessary to make a determination regarding work fitness. For example, the regulation states that the "healthcare professional's written opinion....shall be limited to whether (the appropriate treatment) is indicated for an employee, and if the employee has received such (appropriate treatment)."[2] We believe that Congress should enact a law to protect individually identifiable health information utilizing the standards set forth in the bloodborne pathogens regulations.

To be clear, occupational health professionals have an ethical obligation to safeguard health information confidentiality. AAOHN's ethical tenets caution against inappropriately disclosing confidential information yet recognize, however, that there are a number of appropriate ethical and legal exceptions to the rule. For example, it is perfectly ethical and legal to disclose information concerning threats of homicide, threats of suicide, reportable diseases, child or elder abuse, any injury caused by firearms or other violent acts, and other information covered

---

[1] 29 CFR Ch. XVII (7-1-97 Edition), Section 1910.1030. Bloodborne pathogens.

[2] Id.

by law. Other types of disclosures for specific purposes such as controlled research, emergencies, civil, judicial and administrative purposes, law enforcement, oversight and payment may also be appropriate.

Employers must be able to access certain personal health information when considering pre-placement testing, fitness for work exams and workplace health testing. Specific limited information must be available to employers making reasonable job accommodations in cases of disability or reviewing claims for workers' compensation benefits. In addition, because employers are also responsible for providing a number of other types of benefits such as health and disability insurance, family medical leave and employee assistance programs they may require that certain specific health information be disclosed. AAOHN firmly believes that employers should be allowed to administer these important programs in an efficient manner.

Unfortunately, occupational health nurses are often pressured by employers to release a workers' entire medical record. As such, the occupational health professional is caught between management demands and the nurse's ethical responsibility to protect the employee's confidentiality. Many of our members can attest to the fact that employers often pressure occupational health nurses to divulge the confidential health information of their employees. For too many occupational health nurses this ethical and legal dilemma is not a theoretical issue. The cases of Bettye Jane Gass and Kathleen Easterson provide two such examples:

BETTYE JANE GASS

Bettye Jane Gass became a registered nurse when she passed her Kentucky Nursing Boards in 1975. Shortly thereafter, Ms. Gass began working at both Western Kentucky University and the Lord Corporation on a part-time basis. She later left the employment of Western Kentucky University to become a full-time Health Services Specialist at the Lord Corporation's Bowling Green plant.

In that position Bettye Jane Gass was responsible for providing treatment to employees who sustained injury or became ill. She was also responsible for maintaining the case histories of workers; coordinating paper work flow for injury compensation reports; scheduling pre-employment physicals and follow-up physician visits; preparing summaries and reports; and maintaining OSHA record-keeping requirements as well as coordinating activities of the company's wellness program. She was asked to return to part-time status in 1993 and was terminated on September 7, 1995, without prior notice after approximately thirteen and one-half years at the Lord Corporation.

On that date, the human resource manager demanded access to the routine physical examinations given to all plant employees. Betty Jane Gass refused to turn over the keys to the filing cabinet where the worksite health information was kept. She refused to violate her ethical obligations and despite a written company policy that expressly stated that health

services personnel should maintain confidentiality and provide limited access to the medical files, she was fired for "insubordination." The state court that heard her case issued a summary judgment stating that Ms. Gass "failed to show that her discharge was in violation of any fundamental and well defined public policy as evidenced by a constitutional or statutory provision." Bettye Jane Gass also lost on appeal.

KATHLEEN EASTERSON

In the case of Kathleen Easterson, the issues of employer pressure resulting in the termination of an occupational health nurse are again presented. Kathleen Easterson, an occupational health nurse and Assistant Director of Nursing and Director of Employee Health at a New York area medical center, was terminated by her employer when she refused to disclose the contents of a doctor's note containing an employee's non-occupational diagnosis of severe headache and TMJ trauma. Like the case of Bettye Jane Gass, the termination occurred despite the fact that there was an explicit corporate policy pertaining to medical records confidentiality.

In the court case that followed the hospital's actions, Ms. Easterson sued for wrongful discharge and reinstatement of employment. Ms. Easterson explained to the court that she believed that the worker in her care had a reasonable expectation of privacy with respect to the medical records kept in her care. She believed this to be true because of the existence of the

nurse-client confidential relationship. She explained to the court that the employer's policy and practice of reviewing an employee's medical record without consent should not be tolerated. If employers were allowed to continue this policy, she argued, it would erode trust in the health care system and should therefore, be held to be against the interests of good public policy. Ms. Easterson maintained that the doctor's note was part of the employee's confidential record and that there was no governmental compulsion to reveal the employee's medical record.

Unfortunately, the two lower courts that heard the case held that there was no nurse-client relationship between the occupational health nurse and the employee. In addition, the court held that the doctor's note at issue, was not information acquired by the nurse in attending the employee/client. The court also found that the doctor's note was not necessary to enable the nurse to act in a nurse-client capacity. The court determined that the doctor's note did not create a substantial and specific danger to the public health. Finally, the court determined that there was no basis in law upon which to provide Ms. Easterson with relief for her claims. AAOHN believes that the lack of legal recourse in both the Gass and Easterson cases is egregious and should be corrected through Congressional enactment of comprehensive confidentiality legislation.

GREATER PROTECTIONS SHOULD BE CREATED UNDER FEDERAL LAW

AAOHN maintains that workers must be allowed to feel that their private disclosures will be treated in a dignified and confidential manner. The existence of the patch work of state laws does not always provide such assurances in the worksite setting. Under the laws of many states, employers are not prohibited from accessing detailed personally identifiable employee health information within the company. This is true because the occupational health professional is viewed as an agent of the employer, not as a health care provider with a duty of confidentiality to the patient-employee. In addition, courts have found that physicians representing employers are not bound by the physician-patient duty of confidentiality.[3]

At the same time, health care professionals have been held liable in some states for violations of their professional duty to respect privacy. For example, when a private physician notified an employer that an employee had a "long-standing nervous condition with feelings of anxiety, and insecurity," the patient won an award for damages from the physician because the patient had asked not to have the information released and because the court could find no compelling reason for the disclosure.[4] In another case, the West Virginia Supreme Court held that under

---

[3]Rogers v. Horvath, 237 N.W. 2d 595 (Mich. 1995).

[4]Horne v. Patton, 287 So.2d 824 (Ala. 1974).

the state's workers' compensation statute, physicians can allow employers access to written medical reports but not to information collected from oral communications. The court also ruled that employees can sue both their physicians for releasing confidential information and their employer for requesting the information.[5]

In still other cases, health care professionals have not been held liable in at least one state that has attempted to protect patients from unfair information practices, for arguably the wrong reasons. In *Warner v. Lerner,* 115 Md. App. 428, 693 A.2nd 394 (1997), in an unrelated case, a plaintiff named Leo Kelly, Jr., brought suit against a physician named Dr. Brad Lerner based on medical malpractice. In that case the parties agreed to submit the claim to binding arbitration. The plaintiff hired an expert witness named Dr. Horst Schirmer to testify that Dr. Lerner had breached the standard of care by performing an operation known as a transurethral resection of the prostate ("TURP") on the plaintiff.

On cross-examination, Lerner's counsel sought to impeach Schirmer by introducing a copy of a pathology report that indicated that Dr. Schirmer had performed the identical surgery under conditions he alleged constituted a breach of care on the part of Dr. Learner. The subject of that pathology report was William Warner. In the instant case, Warner sued Learner alleging

---

[5]Morris v. Consolidation Coal, 446 S.E.2d 648 (W.Va. 1994).

that a violation of the Maryland Confidentiality Records Act of 1990, resulted from Lerner's improper taking and using Warner's medical records without his prior consent. Lerner filed a motion to dismiss the case which the Court granted on the grounds that the law stated that "a health care provider may disclose a medical record without the authorization of a person in interest." Despite the fact that the Maryland legislature intended to protect patients from violations of confidential information, they did not foresee that health care providers such as Dr. Lerner would use this loop hole for their own purposes. The Court stated:

> [w]e are troubled here...[d]espite this Court's quite obvious discomfort, maybe even displeasure, or its severe reservations regarding just what was intended by the general assembly, the language of the statute is clear, and we must give meaning to those words as those words set forth by that deliberative body.

This case points out some of the more egregious perils and pitfalls that exist in the current patch work quilt of confidentiality laws.

AAOHN believes that workers must be provided with adequate confidentiality safeguards regardless of where the personally identifiable health information is obtained or maintained. We believe that Congress, therefore, must enact comprehensive uniform medical record confidentiality legislation in order to protect both workers and occupational health professionals. Without an appropriate amount of carefully crafted legal protections, health

care professionals will continue to have difficulty in protecting workers' personal health care information and struggle with the burdens of carrying out their ethical obligations.

THE "CONSUMER PROTECTION AND MEDICAL RECORD CONFIDENTIALITY ACT OF 1998" (H.R. 3900)

The "Consumer Protection and Medical Record Confidentiality Act of 1998" (H.R. 3900), was introduced by Representative Christopher Shays (R-CT) and Thomas Barrett (D-WI) on May 19, 1998. We appreciate both of the Congressman's efforts to advance the debate on this important issue. We are concerned, however, that this new approach to patient confidentiality may not go far enough. The "Consumer Protection and Medical Record Confidentiality Act of 1998" (H.R. 3900) would:

- create a federal right to confidentiality of medical information;

- develop a procedure for patients to authorize the use of their confidential information by insurers, hospitals, researchers and many others including drug manufacturers;

- create civil and criminal penalties for the unauthorized disclosure of individually identifiable health information including potential exclusion from Medicare, Medicaid and other federal health programs; and

- preempt state law except for specific state laws such as mental health, public health, communicable diseases and the reporting of vital statistics, abuse or neglect.

The bill would, in general, prohibit the negligent or intentional disclosure of individually identifiable health information without appropriate authorization. The bill contains a number of provisions that we believe will be helpful to patients and professionals interested in maintaining patient confidentiality. For example, H.R. 3900 require that a notice of confidentiality practices be posted in public.

Unfortunately, the bill also contains so many exceptions to the fundamental rule of confidentiality that the power of this worthwhile prohibition is nearly rendered moot. For example, the bill allows for the disclosure of individually identifiable health information made "to a manufacturer of a drug, biologic, or medical device" (Section 101 (B)(vii)). As other exceptions allow disclosures that are "made to a party to, or potential party to, a merger or acquisition of a commercial enterprise, in anticipation of, or upon, the merger or acquisition" Section 101 (B)(viii). We see no compelling reason to allow unauthorized disclosures of individually identifiable health information for these purposes. In addition, we believe that the quality of health care may actually be compromised by allowing these types of disclosures because patients are likely to be far less forthcoming with the information they provide to health care workers if they know that this material may be made publically available.

While the bill generally preempts state laws, its contains a number of exceptions with respect to state laws regarding mental health, public health, communicable diseases and the reporting of vital statistics, abuse or neglect. We support federal preemption in the area of patient confidentiality yet are intrigued by the bill's treatment of the preemption of specific state laws. Clearly, federal preemption of state laws is one of the most important issues Congress will face regarding patient confidentiality. We look forward to learning more about this novel approach as the bill advances through the House.

Finally, the language of the bill does not expressly address individually identifiable health information that is maintained at the worksite or the important issue of the release of records maintained for the purposes of workers' compensation cases when they are created "within an entity." We stand ready to work with Member's of this Committee and Representatives Shays and Barrett on this important issue.

We commend to your attention, nevertheless, the latest draft version of the "Medical Information Protection Act of 1998," sponsored by Senator Robert Bennett (R-UT) and the "Health Care Personal Information Nondisclosure Act of 1998," (S. 1921) sponsored by Senator James Jeffords (R-VT). We believe that these proposals may offer a more appropriate structure that may best support the basic rule of nondisclosure of individually identifiable health information. As such, these bills will provide greater patient confidentiality and offer a valuable starting point in this debate. AAOHN has indicated its support for a number of

elements contained in the latest draft version of the "Medical Information Protection Act of 1998," sponsored by Senator Robert Bennett. Although this bill has not been introduced, we favor the Bennett approach, especially concerning the issue of preemption. Nevertheless, we believe that both the Bennett proposal and the Jeffords bill would provide sufficient protections without creating unreasonable burdens on participants and providers in the health care system. Both measures prescribe the following federal standards that would:

- provide individuals with access to their own health information and the right to make corrections;

- impose civil and criminal penalties for wrongful disclosure and mishandling of protected medical records;

- limit an individual's personally identifiable health information that could be disclosed without consent to certain specified circumstances (e.g., emergencies, health research conducted by an approved certified institutional review board, fraud and abuse, etc.); and

- require that a notice of confidentiality practices be posted in public.

Although the bills differ on the preemption of state laws, AAOHN prefers the Bennett approach on this important issue. We support providing uniform legal protections across the nation. Without a broad uniformity provision, conflicts will arise due to the fact that it will not always be obvious that a specific state law does provide for "greater protections" than the federal law. While we believe enacting a weaker preemption provision would be an improvement over the *status quo*, we maintain that anything less than full preemption would lead to greater litigation and confusion.

In general, AAOHN believes that any bill Congress enacts should define the "term health information" broadly enough to include medical records obtained or maintained at the worksite for purposes other than treatment or payment. We also support requiring entities that create health information to post a notice of their confidentiality practices. The simple practice of posting such a notice, we believe, will allow employees an opportunity to gain a clearer understanding of their rights. It would also provide employees with a better understanding that individuals do, indeed, have the power under the law to take legal action against violators when appropriate.

In addition, we are encouraged by the inclusion of criminal sanctions in all of these measures because we believe it is essential that those who would knowingly and intentionally obtain personally identifiable health information and disclose this information in violation of the

proposed law be penalized.[6] We suggest, however, that these bills and other similar measures could be strengthened by making penalties applicable to those circumstances in which individuals are "attempting" to obtain personally identifiable information for purposes of disclosure. It is not enough, in our view, to merely penalize those who are successful at inappropriately obtaining and disclosing personally identifiable health information. The recent news stories regarding the highly aggressive marketing practices of certain health related corporations remind us that greater protections are essential. The change we propose would improve the bill and serve as a significant deterrent against inappropriate disclosures.

Finally, AAOHN is actively working to ensure that any legislation that moves through Congress include a provision that would clarify that the law should not require a health provider within an entity (e.g., a physician or nurse who provides occupational health services) to disclose protected health information to others within the company or entity. This issue is often complicated and steeped in terminology that courts may find unfamiliar. We urge you and others to include in any confidentiality legislation a provision that would protect employee health records related to fitness to work as well as those records that document the treatment of illness or injuries or participation in wellness or employee assistance programs.

---

[6] The "Medical Information Protection Act of 1998," Title III, Subtitle A, Section 301(a).

While we prefer that this important concept be included in actual legislative language, we want to also offer the following suggested Report language:

> "The Committee believes that the health provider who creates or originates the health information within the entity is the proper person to determine whether a disclosure is consistent with the limitations under subsection (d). The intent is to protect the confidentiality of an individual's medical records in the workplace, especially those related to an employee's fitness to work (e.g., medical surveillance records, health screening, return-to-work physical examination records)."

In summary, we believe this type of language would limit the releases of important information to protect employee confidentiality while allowing employers to operate their worksite health programs appropriately.

CONCLUSION

Mr. Chairman, AAOHN greatly appreciates this opportunity to offer our comments for the hearing record. In addition to our specific comments, we offer the following four principles that we believe will be useful as Congress deliberates on this important issue:

First, define health information broadly enough to include all medical records obtained or maintained at the worksite for purposes other than treatment or payment;

Second, require entities that create health information post a notice of their confidentiality practices;

Third, apply the guiding principles of compatibility of purpose and minimal disclosure to all personally identifiable health information available to an employer regardless of the reason why the employer holds or has access to the records;

Fourth, recognize that the health care professional who creates or originates the health information is the appropriate person, rather than management, to determine whether a disclosure is consistent with the purposes underlying the reason for the release of the information;

Lastly, include penalties for coercing or attempting to coerce inappropriate record disclosures as well as penalties for actual misuse.

These elements are essential components of any comprehensive federal medical records confidentiality law intended to protect the personal health information of America's workforce.

We urge Congress to keep principles in mind when legislating and look forward to working with you and your colleagues as this important matter moves through the process.

Testimony of IMS HEALTH

Before the

Subcommittee on Government Management, Information and Technology

of the

House Committee on Government Reform and Oversight

May 19, 1998

For the Written Record

Mr. Chairman and Members of the Subcommittee, IMS HEALTH appreciates this opportunity to share its expertise in protecting patient privacy and to provide specific comments on the Consumer Protection and Medical Record Confidentiality Act of 1998. We commend the Subcommittee for its interest in this issue and support the efforts of Representative Shays in crafting legislation that seeks to protect patient privacy in the most effective way without impeding the progress of health care.

IMS HEALTH – An Overview

IMS HEALTH is the world's leading provider of information, research and analysis to the pharmaceutical and health care industries, with data collection activities in over 90 countries. Founded in 1954, IMS HEALTH operates throughout Europe and is well versed in the requirements of the EU Directive on privacy. In the United States alone, the company collects information from over 250,000 sources: pharmaceutical wholesalers, pharmacies, physicians, hospitals, and clinics and processes over 72 billion records each month.

IMS HEALTH's business includes tracking diseases, treatments and their outcomes, a component of which entails measuring the prescription activities of physicians and the sale of pharmaceutical products. The company tracks billions of anonymized prescription records annually. These data are essential to effective implementation of prescription drug recall programs, performance of pharmaceutical market analyses, assessment of drug utilization patterns (i.e., on- and off-label uses and regional variations in prescribing behavior), and comparison of drug costs.

The company's tracking of disease incidences and physician treatment patterns enables it to develop complex, patient-level databases. These information tools assist the medical, scientific, and health care management communities in conducting outcomes research, implementing best practices, and applying health economic analyses.

Our Commitment to Privacy

Because the collection of medical information touches on one of the most sensitive of all topics, IMS HEALTH has operated with long-standing comprehensive practices to protect the privacy of individuals and preserve the confidentiality of the information we collect. In the U.S., these practices include: requiring that data be anonymized prior to being sent to IMS HEALTH; screening records before acceptance to ensure that they comply with this requirement; tightly controlling access to data; requiring informed patient consent before collecting any personally identifiable information; restricting use of information; routinely auditing information practices; and entering into confidentiality agreements with data sources, employees, and clients. IMS HEALTH's U.S. Code of Fair Information Practices is outlined in greater detail in Attachment A.

An Illustration of IMS HEALTH's U.S. Information Flow

The way in which prescription drug sales data flow to and through IMS HEALTH illustrates the company's privacy practices in operation.

IMS HEALTH's National Prescription Audit™ service provides the most comprehensive measurement of prescription pharmaceuticals dispensed in the U.S. The service captures anonymized prescription activity from all major distribution channels, including chain and independent pharmacies, hospitals, nursing homes, HMOs, clinics, mail order, and other outlets.

All data sources (i.e., wholesalers, chain warehouses, mail order firms, government programs) transmit requested data elements to IMS HEALTH via electronic or hard-copy media. **However, prior to transmission, IMS HEALTH instructs the data suppliers to strip the data of patient identifiers.** These identifiers include name, address, Social Security number, telephone number, and other similar identifiers unique to a particular individual. A random number is assigned to each record for data management purposes only, not for any identification purposes regarding subsequent disclosures of information. The key that can link the random number to a particular individual is held by the data source or a neutral third party outside the data collection process. IMS HEALTH never has access to the key.

IMS HEALTH enters into contractual agreements with its data suppliers, which explain the uses for the data collected. These agreements also include provisions for auditing supplier practices, protecting the integrity of the data collection system, and providing a means for addressing non-compliance.

Once the data are transmitted to IMS HEALTH, they are subject to its screening and validation procedures. These procedures check records for compliance with the anonymization requirement before they are passed into any central database. Data that do

not pass this screen are rejected, with immediate notification to the data supplier and discontinuance of further submissions by that supplier until compliance with the anonymization requirement is confirmed.

As a further preventive measure against IMS HEALTH handling individually identifiable data, the database design for this system has no provisions for storing name, address, phone number, or SSN. In addition to technical controls, all employees sign a confidentiality agreement requiring them to abide by the company's confidentiality policies.

Four Essential Legislative Elements

The IMS HEALTH model can serve as a partial framework for federal legislation aimed at ensuring patient privacy. IMS HEALTH believes that the following four elements should be essential components of any such legislation:

1) **Encourage the use of anonymized data;**
2) **Prohibit "reverse engineering;"**
3) **Require patient consent for the use of patient-identifiable information, with few exceptions;** and
4) **Harmonize state laws through federal preemption.**

Anonymization

Patients are afforded the greatest protection if their information is stripped of personal identifiers. The most effective way to encourage the use of anonymized data is by incorporating practical definitions of "individually identifiable health information" and "anonymized information;" allowing disclosure of individually identifiable information, without consent, for the sole purpose of rendering data anonymized; and permitting the handling and use of anonymized information without patient consent.

The definitions and treatment of "individually identifiable health information" and "anonymized information" in Rep. Shays' legislation restrict the use of patient information when it provides a direct means of identifying an individual but allow such use when personal identifiers have been removed, encrypted, or replaced with a code (and the information is not accompanied by an encryption key). Conversely, other legislation, including S. 1921, introduced by Senators Jeffords and Dodd, provides that in order for information to be deemed "anonymized" and therefore not subject to consent requirements, there must be "no reasonable basis to believe that the information could be used" to identify an individual. Such a vague and unworkable standard fails to recognize that there is no way to forecast accurately and "reasonably" the scope and capabilities of future technologies. Information technology experts from across the country agree that in the near future, virtually all nonidentifiable or anonymized information could be used, manipulated, or merged with other publicly available databases to identify individuals.

Accordingly, reliance on a reasonable basis standard will prevent the development and use of anonymized data by making anonymization subject to a constantly shifting standard. The most effective safeguard is to protect what is obviously identifiable and prohibit "reverse engineering." The Shays bill takes this approach.

The Shays bill and S. 1921 both properly permit disclosure of individually identifiable health information, without patient consent, for the purpose of rendering it anonymized. Again, it always is more protective of patient privacy to encourage, wherever feasible, the use of anonymized data.

Finally, as long as the information is anonymized, there is no justifiable public policy reason to require patient consent prior to its use. The Shays bill wisely adopts this approach, as do most of the other privacy bills introduced in Congress.

Prohibition Against Reverse Engineering

A necessary means of protecting patient privacy is to specifically prohibit an individual or entity from manipulating a nonidentifiable database in order to identify the subject individuals. Regardless of how restrictive one drafts a definition of "anonymized information," technology eventually may enable someone to convert anonymized data into individually identifiable information without use of a key. There never can be a foolproof definition. Recognizing this, and considering the federal interest in fostering, rather than impeding, health care research, the most protective but workable solution is to prohibit reverse engineering and subject violators to strong civil and criminal penalties. Section 102(b) of the Shays bill does contain a reverse engineering prohibition along with civil and criminal sanctions.

Patient Consent for Use of Identifiable Information

Informed consent means that the patient knows who is collecting the data, with whom it will be shared, and for what purposes. IMS HEALTH's current practices are in compliance with Section 103 of the Shays bill. While we support adoption of federal standards for ensuring informed patient consent, we cannot comment on the extent to which some of the requirements of Section 103, such as the expiration date provision, may adversely affect operations of others in the health care sector.

Whenever a person or entity receives a patient's consent to handle individually identifiable health information, that person or entity should establish and implement written confidentiality and security policies with which its employees, agents, and contractors must comply. But adopting policies and processes alone are not sufficient to address privacy concerns successfully. The entire organization needs to understand their importance and underlying rationale and be fully enlisted in creating and enforcing them. The organization must view privacy protection as necessary to ensuring the ongoing viability of its business and satisfying its larger societal obligations.

Employee training and education are essential to any comprehensive privacy program, since many of the potential failures occur at operational levels that are far removed from the day-to-day scrutiny of senior managers. Informed employees can spot problems readily before they become major breaches. These employees should be in a position to enforce privacy policies and practices with parties outside the organization. Suppliers and customers must understand, accept, and adopt appropriate safeguards against improper use of identifiable information. IMS HEALTH strongly supports the provisions in the Shays bill (Section 101(2)) which require persons and entities to provide for reasonable protections against unlawful disclosures of individually identifiable health information, implement written policies to ensure employee compliance, and enter into contracts with business associates regarding compliance with the law.

IMS HEALTH believes there should be few exceptions to the policy of requiring prior patient consent before allowing use of individually identifiable information. The exceptions listed in the Shays bill appear to be reasonable and appropriate.

State Harmonization

Transmission of electronic information in today's world does not recognize state boundaries and should not be hampered by a patchwork of different state laws and restrictions. The European Union recognized the importance of this issue with the passage of its 1995 Directive, which sets out to harmonize the differing regimes of its Member States. Because information technology is an integral part of interstate commerce, the need for uniformity of standards is greater than ever before. Harmonization through federal preemption of state laws governing medical records privacy is critical. It is our understanding that Senator Bennett's draft legislation contains the strongest federal preemption language, and we support that approach. IMS HEALTH believes that exceptions to federal preemption, if any, should be very narrowly drawn. IMS HEALTH takes no position on whether mental health information merits any greater protection or different treatment than other sensitive health information.

Conclusion

It is imperative that any person or entity handling individually identifiable and/or anonymized health information adopt policies and procedures for ensuring patient privacy. Implementation must include everyone in the data collection chain. Education and constant self-auditing are key to an effective system. Federal legislation, such as that proposed in the "Consumer Protection and Medical Record Confidentiality Act of 1998," will help ensure universal adoption of sound practices and promote public trust.

IMS HEALTH is committed to maintaining the right balance between patient privacy and the uses of information that contribute to the advancement of health. We look forward to working with this Subcommittee and other Members of Congress as you consider legislation in this area.

Code of Fair Information Practices

- Strive to maintain the highest standards of data accuracy.
- Take all reasonable measures to ensure data security by:
  - safeguarding against unauthorized access
  - providing access only to employees with a legitimate need for the data and to customers who agree to our usage restrictions
- Respect the individual's privacy by:
  - explaining to data suppliers the uses to which we will put the data and under what circumstances their identity will be disclosed
  - collecting medical information on personally identifiable patients only with their consent—which can be withdrawn at any time
  - allowing all such patients to, upon reasonable request, examine the data that pertain to them
  - complying with the confidentiality requirements of our data suppliers
- Assure that our data are used appropriately—that is, for making strategic and tactical decisions in advancing health care—by:
  - retaining only that information which is germane to our data services
  - requiring that our customers' usage be consistent with the above purpose
  - prohibiting our customers from passing the information to an outside party, except as specified in our contracts
- Ensure compliance with this Code by:
  - routinely auditing our information practices
  - requiring a non-disclosure agreement from each IMS employee with access to data
  - securing appropriate confidentiality agreements from clients

Attachment A

○